Amazon Inspector - Assessment Report

Full Report

Report generated on 2021-03-22 at 22:38:08 UTC

Assessment Template: CVEs-SecurityBestPractices-NetworkReachability

Assessment Run start: 2021-03-22 at 20:54:44 UTC
Assessment Run end: 2021-03-22 at 21:56:32 UTC

Section 1: Executive Summary

This is an Inspector assessment report for an assessment started on 2021-03-22 20:54:44 UTC for assessment template 'CVEs-SecurityBestPractices-NetworkReachability'. The assessment target included 2 instances, and was tested against 3 Rules Packages.

The assessment target is defined using the following EC2 tags

Key	Value
Inspector	True

The following Rules Packages were assessed. A total of 6 findings were created, with the following distribution by severity:

Rules Package	High	Medium	Low	Informational
Common Vulnerabilities and Exposures-1.1	0	0	0	0
Network Reachability-1.1	0	0	0	6
Security Best Practices-1.0	0	0	0	0

Section 2: What is Tested

This section details the Rules Packages included in this assessment run, and the EC2 instances included in the assessment target.

2.1: Rules Packages - Count: 3

2.1.1: Common Vulnerabilities and Exposures-1.1

Description: The rules in this package help verify whether the EC2 instances in your application are exposed to Common Vulnerabilities and Exposures (CVEs). Attacks can exploit unpatched vulnerabilities to compromise the confidentiality, integrity, or availability of your service or data. The CVE system provides a reference for publicly known information security vulnerabilities and exposures. For more information, see https://cve.mitre.org/. If a particular CVE appears in one of the produced Findings at the end of a completed Inspector assessment, you can search https://cve.mitre.org/ using the CVE's ID (for example, "CVE-2009-0021") to find detailed information about this CVE, its severity, and how to mitigate it.
Provider: Amazon Web Services, Inc.
Version: 1.1

2.1.2: Network Reachability-1.1

Description: These rules analyze the reachability of your instances over the network. Attacks can exploit your instances over the network by accessing services that are listening on open ports. These rules evaluate the security your host configuration in AWS to determine if it allows access to ports and services over the network. For reachable ports and services, the Amazon Inspector findings identify where they can be reached from, and provide guidance on how to restrict access to these ports.
Provider: Amazon Web Services, Inc.
Version: 1.1

2.1.3: Security Best Practices-1.0

Description: The rules in this package help determine whether your systems are configured securely.
Provider: Amazon Web Services, Inc.
Version: 1.0

2.2: Assessment Target - CVEs-SecurityBestPractices-NetworkReachability

2.2.1: EC2 Tags:

The following EC2 tags (Key/Value pairs) were used to define this assessment target.

Key	Value
Inspector	True

2.2.2: Instances - Count 2

Instance ID
i-03504b4f3dbe34cdb
i-09eb79537f912a362

Section 3: Findings Summary

This section lists the rules that generated findings, the severity of the finding, and the number of instances affected. More details about the findings can be found in the "Findings Details" section. Rules that passed on all target instances available during the assessment run are listed in the "Passed Rules" section.

3.1: Findings table - Common Vulnerabilities and Exposures-1.1

No findings were generated for this rules package.

3.2: Findings table - Network Reachability-1.1

Rule	Severity	Failed
TCP port 22 (SSH) is reachable from the internet with no listener on instance	Informational	2
TCP port 443 (HTTPS) is reachable from a Peered VPC with no listener on instance	Informational	1
TCP port 443 (HTTPS) is reachable from the internet with no listener on instance	Informational	1
TCP port 80 (HTTP) is reachable from a Peered VPC with no listener on instance	Informational	1
TCP port 80 (HTTP) is reachable from the internet with no listener on instance	Informational	1

3.3: Findings table - Security Best Practices-1.0

No findings were generated for this rules package.

Section 4: Findings Details

This section details the findings generated in this assessment run, and the instances that generated the finding. If an instance is not listed here, that means it was checked and passed.

4.1: Findings details - Common Vulnerabilities and Exposures-1.1

No findings were generated for this rules package.

4.2: Findings details - Network Reachability-1.1

TCP port 22 (SSH) is reachable from the internet with no listener on instance

Severity
Informational

Description
On this instance, recognized port(s) are reachable from the internet with no process listening on the port.

Recommendation
You can edit the Security Group sg-0c78e31cb8b1cd9c9, sg-00c21070fcf4f6e69, sg-0246f091fec157860 to remove access from the internet on port 22

Failed Instances
i-09eb79537f912a362
i-03504b4f3dbe34cdb

TCP port 443 (HTTPS) is reachable from a Peered VPC with no listener on instance

Severity
Informational

Description

On this instance, recognized port(s) are reachable from a Peered VPC with no process listening on the port.

Recommendation
You can edit the Security Group sg-00c21070fcf4f6e69 to remove access from a Peered VPC on port 443

Failed Instances
i-09eb79537f912a362

TCP port 443 (HTTPS) is reachable from the internet with no listener on instance

Severity
Informational

Description
On this instance, recognized port(s) are reachable from the internet with no process listening on the port.

Recommendation
You can edit the Security Group sg-00c21070fcf4f6e69 to remove access from the internet on port 443

Failed Instances
i-09eb79537f912a362

TCP port 80 (HTTP) is reachable from a Peered VPC with no listener on instance

Severity
Informational

Description
On this instance, recognized port(s) are reachable from a Peered VPC with no process listening on the port.

Recommendation
You can edit the Security Group sg-00c21070fcf4f6e69 to remove access from a Peered VPC on port 80

Failed Instances
i-09eb79537f912a362

TCP port 80 (HTTP) is reachable from the internet with no listener on instance

Severity
Informational

Description
On this instance, recognized port(s) are reachable from the internet with no process listening on the port.

Recommendation
You can edit the Security Group sg-00c21070fcf4f6e69 to remove access from the internet on port 80

Failed Instances
i-09eb79537f912a362

4.3: Findings details - Security Best Practices-1.0

No findings were generated for this rules package.

Section 5: Passed Rules

This section lists the rules that were checked as part of this assessment, and passed on all instances in the assessment target that were available during the assessment run.

5.1 Passed rules - Common Vulnerabilities and Exposures-1.1

Rule	Description
CVE-2009-0114	Unspecified vulnerability in the Settings Manager in Adobe Flash Player 9.x before 9.0.159.0 and 10.x before 10.0.22.87, and possibly other versions, allows remote attackers to trick a user into visiting an arbitrary URL via unknown vectors, related to "a potential Clickjacking issue variant."
CVE-2009-0198	Heap-based buffer overflow in the JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted PDF file that contains JBIG2 text region segments with Huffman encoding.
CVE-2009-0276	Cross-domain vulnerability in the V8 JavaScript engine in Google Chrome before 1.0.154.46 allows remote attackers to bypass the Same Origin Policy via a crafted script that accesses another frame and reads its full URL and possibly other sensitive information, or modifies the URL of this frame.
CVE-2009-0509	Heap-based buffer overflow in the JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 allows remote attackers to execute arbitrary code via a crafted file that triggers memory corruption.
CVE-2009-0510	Heap-based buffer overflow in the JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-0511, CVE-2009-0512, CVE-2009-0888, and CVE-2009-0889.

CVE-2009-0511	Heap-based buffer overflow in the JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-0510, CVE-2009-0512, CVE-2009-0888, and CVE-2009-0889.
CVE-2009-0512	Heap-based buffer overflow in the JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-0510, CVE-2009-0511, CVE-2009-0888, and CVE-2009-0889.
CVE-2009-0519	Unspecified vulnerability in Adobe Flash Player 9.x before 9.0.159.0 and 10.x before 10.0.22.87 allows remote attackers to cause a denial of service (browser crash) or possibly execute arbitrary code via a crafted Shockwave Flash (aka .swf) file.
CVE-2009-0520	Adobe Flash Player 9.x before 9.0.159.0 and 10.x before 10.0.22.87 does not properly remove references to destroyed objects during Shockwave Flash file processing, which allows remote attackers to execute arbitrary code via a crafted file, related to a "buffer overflow issue."
CVE-2009-0521	Untrusted search path vulnerability in Adobe Flash Player 9.x before 9.0.159.0 and 10.x before 10.0.22.87 on Linux allows local users to obtain sensitive information or gain privileges via a crafted library in a directory contained in the RPATH.
CVE-2009-0658	Buffer overflow in Adobe Reader 9.0 and earlier, and Acrobat 9.0 and earlier, allows remote attackers to execute arbitrary code via a crafted PDF document, related to a non-JavaScript function call and possibly an embedded JBIG2 image stream, as exploited in the wild in February 2009 by Trojan.Pidief.E.
CVE-2009-0888	Heap-based buffer overflow in the JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-0510, CVE-2009-0511, CVE-2009-0512, and CVE-2009-0889.
CVE-2009-0889	Heap-based buffer overflow in the JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow

	remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-0510, CVE-2009-0511, CVE-2009-0512, and CVE-2009-0888.
CVE-2009-0945	Array index error in the insertItemBefore method in WebKit, as used in Apple Safari before 3.2.3 and 4 Public Beta, iPhone OS 1.0 through 2.2.1, iPhone OS for iPod touch 1.1 through 2.2.1, Google Chrome Stable before 1.0.154.65, and possibly other products allows remote attackers to execute arbitrary code via a document with a SVGPathList data structure containing a negative index in the (1) SVGTransformList, (2) SVGStringList, (3) SVGNumberList, (4) SVGPathSegList, (5) SVGPointList, or (6) SVGLengthList SVGList object, which triggers memory corruption.
CVE-2009-1412	Argument injection vulnerability in the chromehtml: protocol handler in Google Chrome before 1.0.154.59, when invoked by Internet Explorer, allows remote attackers to determine the existence of files, and open tabs for URLs that do not satisfy the IsWebSafeScheme restriction, via a web page that sets document.location to a chromehtml: value, as demonstrated by use of a (1) javascript: or (2) data: URL. NOTE: this can be leveraged for Universal XSS by exploiting certain behavior involving persistence across page transitions.
CVE-2009-1441	Heap-based buffer overflow in the ParamTraits<SkBitmap>::Read function in Google Chrome before 1.0.154.64 allows attackers to leverage renderer access to cause a denial of service (application crash) or possibly execute arbitrary code via vectors related to a large bitmap that arrives over the IPC channel.
CVE-2009-1442	Multiple integer overflows in Skia, as used in Google Chrome 1.x before 1.0.154.64 and 2.x, and possibly Android, might allow remote attackers to execute arbitrary code in the renderer process via a crafted (1) image or (2) canvas.
CVE-2009-1492	The getAnnots Doc method in the JavaScript API in Adobe Reader and Acrobat 9.1, 8.1.4, 7.1.1, and earlier allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via a PDF file that contains an annotation, and has an OpenAction entry with JavaScript code that calls this method with crafted integer arguments.
CVE-2009-1493	The customDictionaryOpen spell method in the JavaScript API in Adobe Reader 9.1, 8.1.4, 7.1.1, and earlier on Linux and UNIX allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via a PDF file that triggers a

	call to this method with a long string in the second argument.
CVE-2009-1690	Use-after-free vulnerability in WebKit, as used in Apple Safari before 4.0, iPhone OS 1.0 through 2.2.1, iPhone OS for iPod touch 1.1 through 2.2.1, Google Chrome 1.0.154.53, and possibly other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) by setting an unspecified property of an HTML tag that causes child elements to be freed and later accessed when an HTML error occurs, related to "recursion in certain DOM event handlers."
CVE-2009-1855	Stack-based buffer overflow in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow attackers to execute arbitrary code via a PDF file containing a malformed U3D model file with a crafted extension block.
CVE-2009-1856	Integer overflow in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 allows attackers to cause a denial of service or possibly execute arbitrary code via a PDF file containing unspecified parameters to the FlateDecode filter, which triggers a heap-based buffer overflow.
CVE-2009-1857	Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 allow attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a PDF document with a crafted TrueType font.
CVE-2009-1858	The JBIG2 filter in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow remote attackers to execute arbitrary code via unspecified vectors that trigger memory corruption.
CVE-2009-1859	Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow attackers to execute arbitrary code via unspecified vectors that trigger memory corruption.
CVE-2009-1861	Multiple heap-based buffer overflows in Adobe Reader 7 and Acrobat 7 before 7.1.3, Adobe Reader 8 and Acrobat 8 before 8.1.6, and Adobe Reader 9 and Acrobat 9 before 9.1.2 might allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted PDF file with a JPX (aka JPEG2000) stream that triggers heap memory corruption.

CVE-2009-1862	Unspecified vulnerability in Adobe Reader and Acrobat 9.x through 9.1.2, and Adobe Flash Player 9.x through 9.0.159.0 and 10.x through 10.0.22.87, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via (1) a crafted Flash application in a .pdf file or (2) a crafted .swf file, related to authplay.dll, as exploited in the wild in July 2009.
CVE-2009-1864	Heap-based buffer overflow in Adobe Flash Player before 9.0.246.0 and 10.x before 10.0.32.18, and Adobe AIR before 1.5.2, allows attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unspecified vectors.
CVE-2009-1865	Adobe Flash Player before 9.0.246.0 and 10.x before 10.0.32.18, and Adobe AIR before 1.5.2, allows attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unspecified vectors, related to a "null pointer vulnerability."
CVE-2009-1866	Stack-based buffer overflow in Adobe Flash Player before 9.0.246.0 and 10.x before 10.0.32.18, and Adobe AIR before 1.5.2, allows attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unspecified vectors.
CVE-2009-1867	Adobe Flash Player before 9.0.246.0 and 10.x before 10.0.32.18, and Adobe AIR before 1.5.2, allows attackers to trick a user into (1) selecting a link or (2) completing a dialog, related to a "clickjacking vulnerability."
CVE-2009-1868	Heap-based buffer overflow in Adobe Flash Player before 9.0.246.0 and 10.x before 10.0.32.18, and Adobe AIR before 1.5.2, allows attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unspecified vectors involving URL parsing.
CVE-2009-1869	Integer overflow in the ActionScript Virtual Machine 2 (AVM2) abcFile parser in Adobe Flash Player before 9.0.246.0 and 10.x before 10.0.32.18, and Adobe AIR before 1.5.2, allows attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an AVM2 file with a large intrf_count value that triggers a dereference of an out-of-bounds pointer.
CVE-2009-1870	Adobe Flash Player before 9.0.246.0 and 10.x before 10.0.32.18, and Adobe AIR before 1.5.2, allows attackers to obtain sensitive information via vectors involving saving an SWF file to a hard drive, related to a "local sandbox vulnerability."
CVE-2009-2121	Buffer overflow in the browser kernel in Google Chrome before 2.0.172.33 allows remote HTTP servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted response.

CVE-2009-2555	Heap-based buffer overflow in src/jsregexp.cc in Google V8 before 1.1.10.14, as used in Google Chrome before 2.0.172.37, allows remote attackers to execute arbitrary code in the Chrome sandbox via a crafted JavaScript regular expression.
CVE-2009-2556	Google Chrome before 2.0.172.37 allows attackers to leverage renderer access to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unspecified vectors that trigger excessive memory allocation.
CVE-2009-2564	NOS Microsystems getPlus Download Manager, as used in Adobe Reader 1.6.2.36 and possibly other versions, Corel getPlus Download Manager before 1.5.0.48, and possibly other products, installs NOS\bin\getPlus_HelperSvc.exe with insecure permissions (Everyone:Full Control), which allows local users to gain SYSTEM privileges by replacing getPlus_HelperSvc.exe with a Trojan horse program, as demonstrated by use of getPlus Download Manager within Adobe Reader. NOTE: within Adobe Reader, the scope of this issue is limited because the program is deleted and the associated service is not automatically launched after a successful installation and reboot.
CVE-2009-2935	Google V8, as used in Google Chrome before 2.0.172.43, allows remote attackers to bypass intended restrictions on reading memory, and possibly obtain sensitive information or execute arbitrary code in the Chrome sandbox, via crafted JavaScript.
CVE-2009-2973	Google Chrome before 2.0.172.43 does not prevent SSL connections to a site with an X.509 certificate signed with the (1) MD2 or (2) MD4 algorithm, which makes it easier for man-in-the-middle attackers to spoof arbitrary HTTPS servers via a crafted certificate, a related issue to CVE-2009-2409.
CVE-2009-2979	Adobe Reader and Acrobat 9.x before 9.2, 8.x before 8.1.7, and possibly 7.x through 7.1.4 do not properly perform XMP-XML entity expansion, which allows remote attackers to cause a denial of service via a crafted document.
CVE-2009-2980	Integer overflow in Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 allows attackers to cause a denial of service or possibly execute arbitrary code via unspecified vectors.
CVE-2009-2981	Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 do not properly validate input, which might allow attackers to bypass intended Trust Manager restrictions via unspecified vectors.
CVE-2009-2982	An unspecified certificate in Adobe Reader and Acrobat 9.x before 9.2, 8.x before 8.1.7, and possibly 7.x

	through 7.1.4 might allow remote attackers to conduct a "social engineering attack" via unknown vectors.
CVE-2009-2983	Adobe Reader and Acrobat 9.x before 9.2, 8.x before 8.1.7, and possibly 7.x through 7.1.4 allow attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.
CVE-2009-2984	Unspecified vulnerability in the image decoder in Adobe Acrobat 9.x before 9.2, and possibly 7.x through 7.1.4 and 8.x through 8.1.7, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors.
CVE-2009-2985	Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 allow attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-2996.
CVE-2009-2986	Multiple heap-based buffer overflows in Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 might allow attackers to execute arbitrary code via unspecified vectors.
CVE-2009-2988	Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 do not properly validate input, which allows attackers to cause a denial of service via unspecified vectors.
CVE-2009-2989	Integer overflow in Adobe Acrobat 9.x before 9.2, 8.x before 8.1.7, and possibly 7.x through 7.1.4 might allow attackers to execute arbitrary code via unspecified vectors.
CVE-2009-2990	Array index error in Adobe Reader and Acrobat 9.x before 9.2, 8.x before 8.1.7, and possibly 7.x through 7.1.4 might allow attackers to execute arbitrary code via unspecified vectors.
CVE-2009-2991	Unspecified vulnerability in the Mozilla plug-in in Adobe Reader and Acrobat 8.x before 8.1.7, and possibly 7.x before 7.1.4 and 9.x before 9.2, might allow remote attackers to execute arbitrary code via unknown vectors.
CVE-2009-2992	An unspecified ActiveX control in Adobe Reader and Acrobat 9.x before 9.2, 8.x before 8.1.7, and possibly 7.x through 7.1.4 does not properly validate input, which allows attackers to cause a denial of service via unknown vectors.
CVE-2009-2993	The JavaScript for Acrobat API in Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 does not properly implement the (1) Privileged Context and (2) Safe Path restrictions for unspecified JavaScript methods, which allows remote attackers to create arbitrary files, and possibly execute arbitrary code, via the cPath parameter in a crafted PDF

	file. NOTE: some of these details are obtained from third party information.
CVE-2009-2994	Buffer overflow in Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 might allow attackers to execute arbitrary code via unspecified vectors.
CVE-2009-2996	Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 allow attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-2985.
CVE-2009-2997	Heap-based buffer overflow in Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 might allow attackers to execute arbitrary code via unspecified vectors.
CVE-2009-2998	Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 do not properly validate input, which might allow attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-3458.
CVE-2009-3263	Cross-site scripting (XSS) vulnerability in Google Chrome 2.x and 3.x before 3.0.195.21 allows remote attackers to inject arbitrary web script or HTML via a (1) RSS or (2) Atom feed, related to the rendering of the application/rss+xml content type as XML "active content."
CVE-2009-3264	The getSVGDocument method in Google Chrome before 3.0.195.21 omits an unspecified "access check," which allows remote web servers to bypass the Same Origin Policy and conduct cross-site scripting attacks via unknown vectors, related to a user's visit to a different web server that hosts an SVG document.
CVE-2009-3431	Stack consumption vulnerability in Adobe Reader and Acrobat 9.1.3, 9.1.2, 9.1.1, and earlier 9.x versions; 8.1.6 and earlier 8.x versions; and possibly 7.1.4 and earlier 7.x versions allows remote attackers to cause a denial of service (application crash) via a PDF file with a large number of [(open square bracket) characters in the argument to the alert method. NOTE: some of these details are obtained from third party information.
CVE-2009-3458	Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 do not properly validate input, which might allow attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2009-2998.
CVE-2009-3459	Heap-based buffer overflow in Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 allows remote attackers to execute arbitrary code via a crafted PDF file that triggers memory corruption, as exploited in the wild in October 2009.

	NOTE: some of these details are obtained from third party information.
CVE-2009-3460	Adobe Acrobat 9.x before 9.2, 8.x before 8.1.7, and possibly 7.x through 7.1.4 allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.
CVE-2009-3461	Unspecified vulnerability in Adobe Acrobat 9.x before 9.2 allows attackers to bypass intended file-extension restrictions via unknown vectors.
CVE-2009-3462	Adobe Reader and Acrobat 7.x before 7.1.4, 8.x before 8.1.7, and 9.x before 9.2 on Unix, when Debug mode is enabled, allow attackers to execute arbitrary code via unspecified vectors, related to a "format bug."
CVE-2009-3467	Cross-site scripting (XSS) vulnerability in an unspecified method in Adobe ColdFusion 8.0, 8.0.1, and 9.0 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.
CVE-2009-3793	Unspecified vulnerability in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory consumption) or possibly execute arbitrary code via unknown vectors.
CVE-2009-3794	Heap-based buffer overflow in Adobe Flash Player before 10.0.42.34 and Adobe AIR before 1.5.3 allows remote attackers to execute arbitrary code via crafted dimensions of JPEG data in an SWF file.
CVE-2009-3796	Adobe Flash Player before 10.0.42.34 and Adobe AIR before 1.5.3 might allow attackers to execute arbitrary code via unspecified vectors, related to a "data injection vulnerability."
CVE-2009-3797	Adobe Flash Player 10.x before 10.0.42.34 and Adobe AIR before 1.5.3 might allow attackers to execute arbitrary code via unspecified vectors that trigger memory corruption.
CVE-2009-3798	Adobe Flash Player before 10.0.42.34 and Adobe AIR before 1.5.3 might allow attackers to execute arbitrary code via unspecified vectors that trigger memory corruption.
CVE-2009-3799	Integer overflow in the Verifier::parseExceptionHandlers function in Adobe Flash Player before 10.0.42.34 and Adobe AIR before 1.5.3 allows remote attackers to execute arbitrary code via an SWF file with a large exception_count value that triggers memory corruption, related to "generation of ActionScript exception handlers."
CVE-2009-3800	Multiple unspecified vulnerabilities in Adobe Flash Player before 10.0.42.34 and Adobe AIR before 1.5.3 allow attackers to cause a denial of service (application

	crash) or possibly execute arbitrary code via unknown vectors.
CVE-2009-3931	Incomplete blacklist vulnerability in browser/download/download_exe.cc in Google Chrome before 3.0.195.32 allows remote attackers to force the download of certain dangerous files via a "Content-Disposition: attachment" designation, as demonstrated by (1) .mht and (2) .mhtml files, which are automatically executed by Internet Explorer 6; (3) .svg files, which are automatically executed by Safari; (4) .xml files; (5) .htt files; (6) .xsl files; (7) .xslt files; and (8) image files that are forbidden by the victim's site policy.
CVE-2009-3932	The Gears plugin in Google Chrome before 3.0.195.32 allows user-assisted remote attackers to cause a denial of service (memory corruption and plugin crash) or possibly execute arbitrary code via unspecified use of the Gears SQL API, related to putting "SQL metadata into a bad state."
CVE-2009-3933	WebKit before r50173, as used in Google Chrome before 3.0.195.32, allows remote attackers to cause a denial of service (CPU consumption) via a web page that calls the JavaScript setInterval method, which triggers an incompatibility between the WTF::currentTime and base::Time functions.
CVE-2009-3934	The WebFrameLoaderClient::dispatchDidChangeLocationWithinPage function in src/webkit/glue/webframeloaderclient_impl.cc in Google Chrome before 3.0.195.32 allows user-assisted remote attackers to cause a denial of service via a page-local link, related to an "empty redirect chain," as demonstrated by a message in Yahoo! Mail.
CVE-2009-5072	Memory leak in the ldap_explode_dn function in IBM Tivoli Directory Server (TDS) 6.0 before 6.0.0.61 (aka 6.0.0.8-TIV-ITDS-IF0003) allows remote authenticated users to cause a denial of service (memory consumption) via an empty string argument.
CVE-2009-5073	IBM Tivoli Directory Server (TDS) 6.0 before 6.0.0.59 (aka 6.0.0.8-TIV-ITDS-IF0001) allows remote authenticated users to cause a denial of service (infinite loop and daemon hang) by adding a nested group that contains the Distinguished Name (DN) of its parent entry.
CVE-2010-0185	The default configuration of Adobe ColdFusion 9.0 does not restrict access to collections that have been created by the Solr Service, which allows remote attackers to obtain collection metadata, search information, and index data via a request to an unspecified URL.
CVE-2010-0186	Cross-domain vulnerability in Adobe Flash Player before 10.0.45.2, Adobe AIR before 1.5.3.9130, and

	Adobe Reader and Acrobat 8.x before 8.2.1 and 9.x before 9.3.1 allows remote attackers to bypass intended sandbox restrictions and make cross-domain requests via unspecified vectors.
CVE-2010-0187	Adobe Flash Player before 10.0.45.2 and Adobe AIR before 1.5.3.9130 allow remote attackers to cause a denial of service (application crash) via a modified SWF file.
CVE-2010-0190	Cross-site scripting (XSS) vulnerability in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2010-0191	Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allow attackers to execute arbitrary code via unspecified vectors, related to a "prefix protocol handler vulnerability."
CVE-2010-0192	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2010-0193 and CVE-2010-0196.
CVE-2010-0193	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2010-0192 and CVE-2010-0196.
CVE-2010-0194	Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allow attackers to cause a denial of service (memory corruption) or execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0197, CVE-2010-0201, and CVE-2010-0204.
CVE-2010-0195	Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, do not properly handle fonts, which allows attackers to execute arbitrary code via unspecified vectors.
CVE-2010-0196	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2010-0192 and CVE-2010-0193.
CVE-2010-0197	Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allow attackers to cause a denial of service (memory corruption) or execute arbitrary code via unspecified

	vectors, a different vulnerability than CVE-2010-0194, CVE-2010-0201, and CVE-2010-0204.
CVE-2010-0198	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0199, CVE-2010-0202, and CVE-2010-0203.
CVE-2010-0199	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0198, CVE-2010-0202, and CVE-2010-0203.
CVE-2010-0201	Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allow attackers to cause a denial of service (memory corruption) or execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0194, CVE-2010-0197, and CVE-2010-0204.
CVE-2010-0202	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0198, CVE-2010-0199, and CVE-2010-0203.
CVE-2010-0203	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0198, CVE-2010-0199, and CVE-2010-0202.
CVE-2010-0204	Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allow attackers to cause a denial of service (memory corruption) or execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0194, CVE-2010-0197, and CVE-2010-0201.
CVE-2010-0209	Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2213, CVE-2010-2214, and CVE-2010-2216.
CVE-2010-0315	WebKit before r53607, as used in Google Chrome before 4.0.249.89, allows remote attackers to discover a redirect's target URL, for the session of a specific user of a web site, by placing the site's URL in the HREF attribute of a stylesheet LINK element, and then

	reading the document.styleSheets[0].href property value, related to an IFRAME element.
CVE-2010-0556	browser/login/login_prompt.cc in Google Chrome before 4.0.249.89 populates an authentication dialog with credentials that were stored by Password Manager for a different web site, which allows user-assisted remote HTTP servers to obtain sensitive information via a URL that requires authentication, as demonstrated by a URL in the SRC attribute of an IMG element.
CVE-2010-0643	Google Chrome before 4.0.249.89 attempts to make direct connections to web sites when all configured proxy servers are unavailable, which allows remote HTTP servers to obtain potentially sensitive information about the identity of a client user via standard HTTP logging, as demonstrated by a proxy server that was configured for the purpose of anonymity.
CVE-2010-0644	Google Chrome before 4.0.249.89, when a SOCKS 5 proxy server is configured, sends DNS queries directly, which allows remote DNS servers to obtain potentially sensitive information about the identity of a client user via request logging, as demonstrated by a proxy server that was configured for the purpose of anonymity.
CVE-2010-0645	Multiple integer overflows in factory.cc in Google V8 before r3560, as used in Google Chrome before 4.0.249.89, allow remote attackers to execute arbitrary code in the Chrome sandbox via crafted use of JavaScript arrays.
CVE-2010-0646	Multiple integer signedness errors in factory.cc in Google V8 before r3560, as used in Google Chrome before 4.0.249.89, allow remote attackers to execute arbitrary code in the Chrome sandbox via crafted use of JavaScript arrays.
CVE-2010-0647	WebKit before r53525, as used in Google Chrome before 4.0.249.89, allows remote attackers to execute arbitrary code in the Chrome sandbox via a malformed RUBY element, as demonstrated by a <ruby>><table><rt> sequence.
CVE-2010-0649	Integer overflow in the CrossCallParamsEx::CreateFromBuffer function in sandbox/src/crosscall_server.cc in Google Chrome before 4.0.249.89 allows attackers to leverage renderer access to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a malformed message, related to deserializing of sandbox messages.
CVE-2010-0650	WebKit, as used in Google Chrome before 4.0.249.78 and Apple Safari, allows remote attackers to bypass intended restrictions on popup windows via crafted use of a mouse click event.

CVE-2010-0651	WebKit before r52784, as used in Google Chrome before 4.0.249.78 and Apple Safari before 4.0.5, permits cross-origin loading of CSS stylesheets even when the stylesheet download has an incorrect MIME type and the stylesheet document is malformed, which allows remote attackers to obtain sensitive information via a crafted document.
CVE-2010-0655	Use-after-free vulnerability in Google Chrome before 4.0.249.78 allows user-assisted remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors involving the display of a blocked popup window during navigation to a different web site.
CVE-2010-0656	WebKit before r51295, as used in Google Chrome before 4.0.249.78, presents a directory-listing page in response to an XMLHttpRequest for a file:/// URL that corresponds to a directory, which allows attackers to obtain sensitive information or possibly have unspecified other impact via a crafted local HTML document.
CVE-2010-0658	Multiple integer overflows in Skia, as used in Google Chrome before 4.0.249.78, allow remote attackers to execute arbitrary code in the Chrome sandbox or cause a denial of service (memory corruption and application crash) via vectors involving CANVAS elements.
CVE-2010-0659	The image decoder in WebKit before r52833, as used in Google Chrome before 4.0.249.78, does not properly handle a failure of memory allocation, which allows remote attackers to execute arbitrary code in the Chrome sandbox via a malformed GIF file that specifies a large size.
CVE-2010-0660	Google Chrome before 4.0.249.78 sends an https URL in the Referer header of an http request in certain circumstances involving https to http redirection, which allows remote HTTP servers to obtain potentially sensitive information via standard HTTP logging.
CVE-2010-0661	WebCore/bindings/v8/custom/V8DOMWindowCustom.cpp in WebKit before r52401, as used in Google Chrome before 4.0.249.78, allows remote attackers to bypass the Same Origin Policy via vectors involving the window.open method.
CVE-2010-0662	The ParamTraits<SkBitmap>::Read function in common/common_param_traits.cc in Google Chrome before 4.0.249.78 does not use the correct variables in calculations designed to prevent integer overflows, which allows attackers to leverage renderer access to cause a denial of service or possibly have unspecified other impact via bitmap data, related to deserialization.
CVE-2010-0663	The ParamTraits<SkBitmap>::Read function in common/common_param_traits.cc in Google Chrome

	before 4.0.249.78 does not initialize the memory locations that will hold bitmap data, which might allow remote attackers to obtain potentially sensitive information from process memory by providing insufficient data, related to use of a (1) thumbnail database or (2) HTML canvas.
CVE-2010-0664	Stack consumption vulnerability in the ChildProcessSecurityPolicy::CanRequestURL function in browser/child_process_security_policy.cc in Google Chrome before 4.0.249.78 allows remote attackers to cause a denial of service (memory consumption and application crash) via a URL that specifies multiple protocols, as demonstrated by a URL that begins with many repetitions of the view-source: substring.
CVE-2010-1228	Multiple race conditions in the sandbox infrastructure in Google Chrome before 4.1.249.1036 have unspecified impact and attack vectors.
CVE-2010-1229	The sandbox infrastructure in Google Chrome before 4.1.249.1036 does not properly use pointers, which has unspecified impact and attack vectors.
CVE-2010-1230	Google Chrome before 4.1.249.1036 does not have the expected behavior for attempts to delete Web SQL Databases and clear the Strict Transport Security (STS) state, which has unspecified impact and attack vectors.
CVE-2010-1231	Google Chrome before 4.1.249.1036 processes HTTP headers before invoking the SafeBrowsing feature, which allows remote attackers to have an unspecified impact via crafted headers.
CVE-2010-1232	Google Chrome before 4.1.249.1036 allows remote attackers to cause a denial of service (memory error) or possibly have unspecified other impact via a malformed SVG document.
CVE-2010-1233	Multiple integer overflows in Google Chrome before 4.1.249.1036 allow remote attackers to have an unspecified impact via vectors involving WebKit JavaScript objects.
CVE-2010-1234	Unspecified vulnerability in Google Chrome before 4.1.249.1036 allows remote attackers to truncate the URL shown in the HTTP Basic Authentication dialog via unknown vectors.
CVE-2010-1235	Unspecified vulnerability in Google Chrome before 4.1.249.1036 allows remote attackers to trigger the omission of a download warning dialog via unknown vectors.
CVE-2010-1236	The protocolIs function in platform/KURLGoogle.cpp in WebCore in WebKit before r55822, as used in Google Chrome before 4.1.249.1036 and Flock Browser 3.x before 3.0.0.4112, does not properly handle whitespace at the beginning of a URL, which allows remote

	attackers to conduct cross-site scripting (XSS) attacks via a crafted javascript: URL, as demonstrated by a \x00javascript:alert sequence.
CVE-2010-1237	Google Chrome 4.1 BETA before 4.1.249.1036 allows remote attackers to cause a denial of service (memory error) or possibly have unspecified other impact via an empty SVG element.
CVE-2010-1240	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, do not restrict the contents of one text field in the Launch File warning dialog, which makes it easier for remote attackers to trick users into executing an arbitrary local program that was specified in a PDF document, as demonstrated by a text field that claims that the Open button will enable the user to read an encrypted message.
CVE-2010-1241	Heap-based buffer overflow in the custom heap management system in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted PDF document, aka FG-VD-10-005.
CVE-2010-1285	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code via unspecified manipulations involving the newclass (0x58) operator and an "invalid pointer vulnerability" that triggers memory corruption, a different vulnerability than CVE-2010-2168 and CVE-2010-2201.
CVE-2010-1293	Cross-site scripting (XSS) vulnerability in the Administrator page in Adobe ColdFusion 8.0, 8.0.1, and 9.0 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2010-1294	Unspecified vulnerability in Adobe ColdFusion 8.0, 8.0.1, and 9.0 allows local users to obtain sensitive information via unknown vectors.
CVE-2010-1295	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2202, CVE-2010-2207, CVE-2010-2209, CVE-2010-2210, CVE-2010-2211, and CVE-2010-2212.
CVE-2010-1297	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64; Adobe AIR before 2.0.2.12610; and Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted SWF content, related to authplay.dll and the ActionScript Virtual

	Machine 2 (AVM2) newfunction instruction, as exploited in the wild in June 2010.
CVE-2010-1487	IBM Lotus Notes 7.0, 8.0, and 8.5 stores administrative credentials in cleartext in SURunAs.exe, which allows local users to obtain sensitive information by examining this file, aka SPR JSTN837SEG.
CVE-2010-1500	Google Chrome before 4.1.249.1059 does not properly support forms, which has unknown impact and attack vectors, related to a "type confusion error."
CVE-2010-1502	Unspecified vulnerability in Google Chrome before 4.1.249.1059 allows remote attackers to access local files via vectors related to "developer tools."
CVE-2010-1503	Cross-site scripting (XSS) vulnerability in Google Chrome before 4.1.249.1059 allows remote attackers to inject arbitrary web script or HTML via vectors related to a chrome://net-internals URI.
CVE-2010-1504	Cross-site scripting (XSS) vulnerability in Google Chrome before 4.1.249.1059 allows remote attackers to inject arbitrary web script or HTML via vectors related to a chrome://downloads URI.
CVE-2010-1505	Google Chrome before 4.1.249.1059 does not prevent pages from loading with the New Tab page's privileges, which has unknown impact and attack vectors.
CVE-2010-1506	The Google V8 bindings in Google Chrome before 4.1.249.1059 allow attackers to cause a denial of service (memory corruption) via unknown vectors.
CVE-2010-1663	The Google URL Parsing Library (aka google-url or GURL) in Google Chrome before 4.1.249.1064 allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2010-1664	Google Chrome before 4.1.249.1064 does not properly handle HTML5 media, which allows remote attackers to cause a denial of service (memory corruption) and possibly have unspecified other impact via unknown vectors.
CVE-2010-1665	Google Chrome before 4.1.249.1064 does not properly handle fonts, which allows remote attackers to cause a denial of service (memory corruption) and possibly have unspecified other impact via unknown vectors.
CVE-2010-1767	Cross-site request forgery (CSRF) vulnerability in loader/DocumentThreadableLoader.cpp in WebCore in WebKit before r57041, as used in Google Chrome before 4.1.249.1059, allows remote attackers to hijack the authentication of unspecified victims via a crafted synchronous preflight XMLHttpRequest operation.
CVE-2010-1770	WebKit in Apple Safari before 5.0 on Mac OS X 10.5 through 10.6 and Windows, Apple Safari before 4.1 on Mac OS X 10.4, and Google Chrome before 5.0.375.70 does not properly handle a transformation of a text

	node that has the IBM1147 character set, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted HTML document containing a BR element, related to a "type checking issue."
CVE-2010-1772	Use-after-free vulnerability in page/Geolocation.cpp in WebCore in WebKit before r59859, as used in Google Chrome before 5.0.375.70, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted web site, related to failure to stop timers associated with geolocation upon deletion of a document.
CVE-2010-1773	Off-by-one error in the toAlphabetic function in rendering/RenderListMarker.cpp in WebCore in WebKit before r59950, as used in Google Chrome before 5.0.375.70, allows remote attackers to obtain sensitive information, cause a denial of service (memory corruption and application crash), or possibly execute arbitrary code via vectors related to list markers for HTML lists, aka rdar problem 8009118.
CVE-2010-1822	WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3 and Google Chrome before 6.0.472.62, does not properly perform a cast of an unspecified variable, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via an SVG element in a non-SVG document.
CVE-2010-1823	Use-after-free vulnerability in WebKit before r65958, as used in Google Chrome before 6.0.472.59, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger use of document APIs such as document.close during parsing, as demonstrated by a Cascading Style Sheets (CSS) file referencing an invalid SVG font, aka rdar problem 8442098.
CVE-2010-1824	Use-after-free vulnerability in WebKit, as used in Apple iTunes before 10.2 on Windows, Apple Safari, and Google Chrome before 6.0.472.59, allows remote attackers to execute arbitrary code or cause a denial of service via vectors related to SVG styles, the DOM tree, and error messages.
CVE-2010-1825	Use-after-free vulnerability in WebKit, as used in Google Chrome before 6.0.472.59, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to nested SVG elements.
CVE-2010-2105	Google Chrome before 5.0.375.55 does not properly follow the Safe Browsing specification's requirements for canonicalization of URLs, which has unspecified impact and remote attack vectors.

CVE-2010-2106	Unspecified vulnerability in Google Chrome before 5.0.375.55 might allow remote attackers to spoof the URL bar via vectors involving unload event handlers.
CVE-2010-2107	Unspecified vulnerability in Google Chrome before 5.0.375.55 allows attackers to cause a denial of service (memory error) or possibly have unspecified other impact via vectors related to the Safe Browsing functionality.
CVE-2010-2108	Unspecified vulnerability in Google Chrome before 5.0.375.55 allows remote attackers to bypass the whitelist-mode plugin blocker via unknown vectors.
CVE-2010-2109	Unspecified vulnerability in Google Chrome before 5.0.375.55 allows user-assisted remote attackers to cause a denial of service (memory error) or possibly have unspecified other impact via vectors related to the "drag + drop" functionality.
CVE-2010-2110	Google Chrome before 5.0.375.55 does not properly execute JavaScript code in the extension context, which has unspecified impact and remote attack vectors.
CVE-2010-2160	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via an invalid offset in an unspecified undocumented opcode in ActionScript Virtual Machine 2, related to getouterscope, a different vulnerability than CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2161	Array index error in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified "types of Adobe Flash code."
CVE-2010-2162	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (heap memory corruption) or possibly execute arbitrary code via vectors related to improper length calculation and the (1) STSC, (2) STSZ, and (3) STCO atoms.
CVE-2010-2163	Multiple unspecified vulnerabilities in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unknown vectors.
CVE-2010-2164	Use-after-free vulnerability in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to

	execute arbitrary code via unspecified vectors related to an unspecified "image type within a certain function."
CVE-2010-2165	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2160, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2166	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2167	Multiple heap-based buffer overflows in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified vectors related to malformed (1) GIF or (2) JPEG data.
CVE-2010-2168	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code via a PDF file with crafted Flash content, involving the newfunction (0x44) operator and an "invalid pointer vulnerability" that triggers memory corruption, a different vulnerability than CVE-2010-1285 and CVE-2010-2201.
CVE-2010-2169	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allow attackers to cause a denial of service (pointer memory corruption) or possibly execute arbitrary code via unspecified vectors.
CVE-2010-2170	Integer overflow in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2181 and CVE-2010-2183.
CVE-2010-2171	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via vectors related to SWF files, decompression of embedded JPEG image data, and the DefineBits and other unspecified tags, a different

	vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2166, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2172	Adobe Flash Player 9 before 9.0.277.0 on unspecified UNIX platforms allows attackers to cause a denial of service via unknown vectors.
CVE-2010-2173	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified vectors, related to an "invalid pointer vulnerability" and the newclass (0x58) operator, a different vulnerability than CVE-2010-2174.
CVE-2010-2174	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified vectors, related to an "invalid pointer vulnerability" and the newfunction (0x44) operator, a different vulnerability than CVE-2010-2173.
CVE-2010-2175	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2176	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2177	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.

CVE-2010-2178	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2179	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, when Firefox or Chrome is used, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors related to URL parsing.
CVE-2010-2180	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2182, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2181	Integer overflow in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2170 and CVE-2010-2183.
CVE-2010-2182	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2183	Integer overflow in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2170 and CVE-2010-2181.
CVE-2010-2184	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different

	vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2185	Buffer overflow in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified vectors.
CVE-2010-2186	Unspecified vulnerability in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2010-2187	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, and CVE-2010-2188.
CVE-2010-2188	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code by calling the ActionScript native object 2200 connect method multiple times with different arguments, a different vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, and CVE-2010-2187.
CVE-2010-2189	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, when used in conjunction with VMWare Tools on a VMWare platform, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.
CVE-2010-2201	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code via a PDF file with crafted Flash content involving the (1) pushstring (0x2C) operator, (2) debugfile (0xF1) operator, and an "invalid pointer vulnerability" that triggers memory corruption, a different vulnerability than CVE-2010-1285 and CVE-2010-2168.
CVE-2010-2202	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow

	attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-1295, CVE-2010-2207, CVE-2010-2209, CVE-2010-2210, CVE-2010-2211, and CVE-2010-2212.
CVE-2010-2203	Adobe Reader and Acrobat 9.x before 9.3.3 on UNIX allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2010-2204	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors.
CVE-2010-2205	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, access uninitialized memory, which allows attackers to execute arbitrary code via unspecified vectors.
CVE-2010-2206	Array index error in AcroForm.api in Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allows remote attackers to execute arbitrary code via a crafted GIF image in a PDF file, which bypasses a size check and triggers a heap-based buffer overflow.
CVE-2010-2207	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-1295, CVE-2010-2202, CVE-2010-2209, CVE-2010-2210, CVE-2010-2211, and CVE-2010-2212.
CVE-2010-2208	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, dereference a heap object after this object's deletion, which allows attackers to execute arbitrary code via unspecified vectors.
CVE-2010-2209	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-1295, CVE-2010-2202, CVE-2010-2207, CVE-2010-2210, CVE-2010-2211, and CVE-2010-2212.
CVE-2010-2210	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-1295, CVE-2010-2202, CVE-2010-2207, CVE-2010-2209, CVE-2010-2211, and CVE-2010-2212.

CVE-2010-2211	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-1295, CVE-2010-2202, CVE-2010-2207, CVE-2010-2209, CVE-2010-2210, and CVE-2010-2212.
CVE-2010-2212	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via a PDF file containing Flash content with a crafted #1023 (3FFh) tag, a different vulnerability than CVE-2010-1295, CVE-2010-2202, CVE-2010-2207, CVE-2010-2209, CVE-2010-2210, and CVE-2010-2211.
CVE-2010-2213	Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-0209, CVE-2010-2214, and CVE-2010-2216.
CVE-2010-2214	Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-0209, CVE-2010-2213, and CVE-2010-2216.
CVE-2010-2215	Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to trick a user into (1) selecting a link or (2) completing a dialog, related to a "click-jacking" issue.
CVE-2010-2216	Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-0209, CVE-2010-2213, and CVE-2010-2214.
CVE-2010-2295	page/EventHandler.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 does not properly handle a change of the focused frame during the dispatching of keydown, which allows user-assisted remote attackers to redirect keystrokes via a crafted HTML document, aka rdar problem 7018610. NOTE: this might overlap CVE-2010-1422.
CVE-2010-2296	The implementation of unspecified DOM methods in Google Chrome before 5.0.375.70 allows remote attackers to bypass the Same Origin Policy via unknown vectors.

CVE-2010-2297	rendering/FixedTableLayout.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an HTML document that has a large colspan attribute within a table.
CVE-2010-2298	browser/renderer_host/database_dispatcher_host.cc in Google Chrome before 5.0.375.70 on Linux does not properly handle ViewHostMsg_DatabaseOpenFile messages in chroot-based sandboxing, which allows remote attackers to bypass intended sandbox restrictions via vectors involving fchdir and chdir calls.
CVE-2010-2299	The Clipboard::DispatchObject function in app/clipboard/clipboard.cc in Google Chrome before 5.0.375.70 does not properly handle CBF_SMBITMAP objects in a ViewHostMsg_ClipboardWriteObjectsAsync message, which might allow remote attackers to execute arbitrary code via vectors involving crafted data from the renderer process, related to a "Type Confusion" issue.
CVE-2010-2300	Use-after-free vulnerability in the Element::normalizeAttributes function in dom/Element.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via vectors related to handlers for DOM mutation events, aka rdar problem 7948784. NOTE: this might overlap CVE-2010-1759.
CVE-2010-2301	Cross-site scripting (XSS) vulnerability in editing/markup.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to inject arbitrary web script or HTML via vectors related to the node.innerHTML property of a TEXTAREA element. NOTE: this might overlap CVE-2010-1762.
CVE-2010-2302	Use-after-free vulnerability in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via vectors involving remote fonts in conjunction with shadow DOM trees, aka rdar problem 8007953. NOTE: this might overlap CVE-2010-1771.
CVE-2010-2455	Opera does not properly manage the address bar between the request to open a URL and the retrieval of the new document's content, which might allow remote attackers to conduct spoofing attacks via a crafted HTML document, a related issue to CVE-2010-1206.
CVE-2010-2645	Unspecified vulnerability in Google Chrome before 5.0.375.99, when WebGL is used, allows remote attackers to cause a denial of service (out-of-bounds read) via unknown vectors.

CVE-2010-2646	Google Chrome before 5.0.375.99 does not properly isolate sandboxed IFRAME elements, which has unspecified impact and remote attack vectors.
CVE-2010-2647	Google Chrome before 5.0.375.99 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via an invalid SVG document.
CVE-2010-2648	The implementation of the Unicode Bidirectional Algorithm (aka Bidi algorithm or UBA) in Google Chrome before 5.0.375.99 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-2649	Unspecified vulnerability in Google Chrome before 5.0.375.99 allows remote attackers to cause a denial of service (application crash) via an invalid image.
CVE-2010-2650	Unspecified vulnerability in Google Chrome before 5.0.375.99 has unknown impact and attack vectors, related to an "annoyance with print dialogs."
CVE-2010-2651	The Cascading Style Sheets (CSS) implementation in Google Chrome before 5.0.375.99 does not properly perform style rendering, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-2652	Google Chrome before 5.0.375.99 does not properly implement modal dialogs, which allows attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2010-2861	Multiple directory traversal vulnerabilities in the administrator console in Adobe ColdFusion 9.0.1 and earlier allow remote attackers to read arbitrary files via the locale parameter to (1) CFIDE/administrator/settings/mappings.cfm, (2) logging/settings.cfm, (3) datasources/index.cfm, (4) j2eepackaging/editarchive.cfm, and (5) enter.cfm in CFIDE/administrator/.
CVE-2010-2862	Integer overflow in CoolType.dll in Adobe Reader 8.2.3 and 9.3.3, and Acrobat 9.3.3, allows remote attackers to execute arbitrary code via a TrueType font with a large maxCompositePoints value in a Maximum Profile (maxp) table.
CVE-2010-2883	Stack-based buffer overflow in CoolType.dll in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a PDF document with a long field in a Smart INdependent Glyphlets (SING) table in a TTF font, as exploited in the wild in September 2010.

	NOTE: some of these details are obtained from third party information.
CVE-2010-2884	Adobe Flash Player 10.1.82.76 and earlier on Windows, Mac OS X, Linux, and Solaris and 10.1.92.10 on Android; authplay.dll in Adobe Reader and Acrobat 9.x before 9.4; and authplay.dll in Adobe Reader and Acrobat 8.x before 8.2.5 on Windows and Mac OS X allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as exploited in the wild in September 2010.
CVE-2010-2887	Multiple unspecified vulnerabilities in Adobe Reader and Acrobat 9.x before 9.4 on Linux allow attackers to gain privileges via unknown vectors.
CVE-2010-2889	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to execute arbitrary code via a crafted font, a different vulnerability than CVE-2010-3626.
CVE-2010-2890	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-3619, CVE-2010-3621, CVE-2010-3622, CVE-2010-3628, CVE-2010-3632, and CVE-2010-3658.
CVE-2010-2897	Google Chrome before 5.0.375.125 does not properly mitigate an unspecified flaw in the Windows kernel, which has unknown impact and attack vectors.
CVE-2010-2898	Google Chrome before 5.0.375.125 does not properly mitigate an unspecified flaw in the GNU C Library, which has unknown impact and attack vectors.
CVE-2010-2899	Unspecified vulnerability in the layout implementation in Google Chrome before 5.0.375.125 allows remote attackers to obtain sensitive information from process memory via unknown vectors.
CVE-2010-2900	Google Chrome before 5.0.375.125 does not properly handle a large canvas, which has unspecified impact and remote attack vectors.
CVE-2010-2901	The rendering implementation in Google Chrome before 5.0.375.125 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-2902	The SVG implementation in Google Chrome before 5.0.375.125 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-2903	Google Chrome before 5.0.375.125 performs unexpected truncation and improper eliding of

	hostnames, which has unspecified impact and remote attack vectors.
CVE-2010-3112	Google Chrome before 5.0.375.127 does not properly implement file dialogs, which allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3113	Google Chrome before 5.0.375.127, and webkitgtk before 1.2.5, does not properly handle SVG documents, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors related to state changes when using DeleteButtonController.
CVE-2010-3114	The text-editing implementation in Google Chrome before 5.0.375.127, and webkitgtk before 1.2.6, does not check a node type before performing a cast, which has unspecified impact and attack vectors related to (1) DeleteSelectionCommand.cpp, (2) InsertLineBreakCommand.cpp, or (3) InsertParagraphSeparatorCommand.cpp in WebCore/editing/.
CVE-2010-3115	Google Chrome before 5.0.375.127, and webkitgtk before 1.2.6, does not properly implement the history feature, which might allow remote attackers to spoof the address bar via unspecified vectors.
CVE-2010-3116	Multiple use-after-free vulnerabilities in WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3, Google Chrome before 5.0.375.127, and webkitgtk before 1.2.6, allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors related to improper handling of MIME types by plug-ins.
CVE-2010-3117	Google Chrome before 5.0.375.127 does not properly implement the notifications feature, which allows remote attackers to cause a denial of service (application crash) and possibly have unspecified other impact via unknown vectors.
CVE-2010-3118	The autosuggest feature in the Omnibox implementation in Google Chrome before 5.0.375.127 does not anticipate entry of passwords, which might allow remote attackers to obtain sensitive information by reading the network traffic generated by this feature.
CVE-2010-3119	Google Chrome before 5.0.375.127 and webkitgtk before 1.2.6 do not properly support the Ruby language, which allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3120	Google Chrome before 5.0.375.127 does not properly implement the Geolocation feature, which allows remote attackers to cause a denial of service (memory

	corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3246	Google Chrome before 6.0.472.53 does not properly handle the _blank value for the target attribute of unspecified elements, which allows remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2010-3247	Google Chrome before 6.0.472.53 does not properly restrict the characters in URLs, which allows remote attackers to spoof the appearance of the URL bar via homographic sequences.
CVE-2010-3248	Google Chrome before 6.0.472.53 does not properly restrict copying to the clipboard, which has unspecified impact and attack vectors.
CVE-2010-3249	Google Chrome before 6.0.472.53 does not properly implement SVG filters, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, related to a "stale pointer" issue.
CVE-2010-3250	Unspecified vulnerability in Google Chrome before 6.0.472.53 allows remote attackers to enumerate the set of installed extensions via unknown vectors.
CVE-2010-3251	The WebSockets implementation in Google Chrome before 6.0.472.53 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via unspecified vectors.
CVE-2010-3252	Use-after-free vulnerability in the Notifications presenter in Google Chrome before 6.0.472.53 allows attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2010-3253	The implementation of notification permissions in Google Chrome before 6.0.472.53 allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3254	The WebSockets implementation in Google Chrome before 6.0.472.53 does not properly handle integer values, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2010-3255	Google Chrome before 6.0.472.53 and webkitgtk before 1.2.6 do not properly handle counter nodes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3256	Google Chrome before 6.0.472.53 does not properly limit the number of stored autocomplete entries, which has unspecified impact and attack vectors.
CVE-2010-3257	Use-after-free vulnerability in WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3, Google

	Chrome before 6.0.472.53, and webkitgtk before 1.2.6, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors involving element focus.
CVE-2010-3258	The sandbox implementation in Google Chrome before 6.0.472.53 does not properly deserialize parameters, which has unspecified impact and remote attack vectors.
CVE-2010-3259	WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3, Google Chrome before 6.0.472.53, and webkitgtk before 1.2.6, does not properly restrict read access to images derived from CANVAS elements, which allows remote attackers to bypass the Same Origin Policy and obtain potentially sensitive image data via a crafted web site.
CVE-2010-3411	Google Chrome before 6.0.472.59 on Linux does not properly handle cursors, which might allow attackers to cause a denial of service (assertion failure) via unspecified vectors.
CVE-2010-3412	Race condition in the console implementation in Google Chrome before 6.0.472.59 has unspecified impact and attack vectors.
CVE-2010-3413	Unspecified vulnerability in the pop-up blocking functionality in Google Chrome before 6.0.472.59 allows remote attackers to cause a denial of service (application crash) via unknown vectors.
CVE-2010-3415	Google Chrome before 6.0.472.59 does not properly implement Geolocation, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3416	Google Chrome before 6.0.472.59 on Linux does not properly implement the Khmer locale, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3417	Google Chrome before 6.0.472.59 does not prompt the user before granting access to the extension history, which allows attackers to obtain potentially sensitive information via unspecified vectors.
CVE-2010-3474	IBM DB2 9.7 before FP3 does not perform the expected drops or invalidations of dependent functions upon a loss of privileges by the functions' owners, which allows remote authenticated users to bypass intended access restrictions via calls to these functions, a different vulnerability than CVE-2009-3471.
CVE-2010-3475	IBM DB2 9.7 before FP3 does not properly enforce privilege requirements for execution of entries in the dynamic SQL cache, which allows remote authenticated

	users to bypass intended access restrictions by leveraging the cache to execute an UPDATE statement contained in a compiled compound SQL statement.
CVE-2010-3619	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2890, CVE-2010-3621, CVE-2010-3622, CVE-2010-3628, CVE-2010-3632, and CVE-2010-3658.
CVE-2010-3620	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to execute arbitrary code via a crafted image, a different vulnerability than CVE-2010-3629.
CVE-2010-3621	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2890, CVE-2010-3619, CVE-2010-3622, CVE-2010-3628, CVE-2010-3632, and CVE-2010-3658.
CVE-2010-3622	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2890, CVE-2010-3619, CVE-2010-3621, CVE-2010-3628, CVE-2010-3632, and CVE-2010-3658.
CVE-2010-3625	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code via unspecified vectors, related to a "prefix protocol handler vulnerability."
CVE-2010-3626	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to execute arbitrary code via a crafted font, a different vulnerability than CVE-2010-2889.
CVE-2010-3627	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to execute arbitrary code via unknown vectors.
CVE-2010-3628	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2890, CVE-2010-3619, CVE-2010-3621, CVE-2010-3622, CVE-2010-3632, and CVE-2010-3658.

CVE-2010-3629	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to execute arbitrary code via a crafted image, a different vulnerability than CVE-2010-3620.
CVE-2010-3630	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors.
CVE-2010-3632	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2890, CVE-2010-3619, CVE-2010-3621, CVE-2010-3622, CVE-2010-3628, and CVE-2010-3658.
CVE-2010-3636	Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, does not properly handle unspecified encodings during the parsing of a cross-domain policy file, which allows remote web servers to bypass intended access restrictions via unknown vectors.
CVE-2010-3639	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors.
CVE-2010-3640	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, CVE-2010-3650, and CVE-2010-3652.
CVE-2010-3641	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3640, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, CVE-2010-3650, and CVE-2010-3652.
CVE-2010-3642	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows,

	Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3640, CVE-2010-3641, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, CVE-2010-3650, and CVE-2010-3652.
CVE-2010-3643	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, CVE-2010-3650, and CVE-2010-3652.
CVE-2010-3644	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3645, CVE-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, CVE-2010-3650, and CVE-2010-3652.
CVE-2010-3645	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, CVE-2010-3650, and CVE-2010-3652.
CVE-2010-3646	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, CVE-2010-3650, and CVE-2010-3652.
CVE-2010-3647	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on

	Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, CVE-2010-3648, CVE-2010-3649, CVE-2010-3650, and CVE-2010-3652.
CVE-2010-3648	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, CVE-2010-3647, CVE-2010-3649, CVE-2010-3650, and CVE-2010-3652.
CVE-2010-3649	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3650, and CVE-2010-3652.
CVE-2010-3650	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, and CVE-2010-3652.
CVE-2010-3652	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, and CVE-2010-3650.
CVE-2010-3654	Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris and 10.1.95.1 on Android, and authplay.dll (aka AuthPlayLib.bundle or libauthplay.so.0.0.0) in Adobe

	Reader and Acrobat 9.x through 9.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via crafted SWF content, as exploited in the wild in October 2010.
CVE-2010-3656	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to cause a denial of service via unknown vectors, a different vulnerability than CVE-2010-3657.
CVE-2010-3657	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to cause a denial of service via unknown vectors, a different vulnerability than CVE-2010-3656.
CVE-2010-3658	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2890, CVE-2010-3619, CVE-2010-3621, CVE-2010-3622, CVE-2010-3628, and CVE-2010-3632.
CVE-2010-3729	The SPDY protocol implementation in Google Chrome before 6.0.472.62 does not properly manage buffers, which might allow remote attackers to execute arbitrary code via unspecified vectors.
CVE-2010-3730	Google Chrome before 6.0.472.62 does not properly use information about the origin of a document to manage properties, which allows remote attackers to have an unspecified impact via a crafted web site, related to a "property pollution" issue.
CVE-2010-3864	Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography.
CVE-2010-4008	libxml2 before 2.7.8, as used in Google Chrome before 7.0.517.44, Apple Safari 5.0.2 and earlier, and other products, reads from invalid memory locations during processing of malformed XPath expressions, which allows context-dependent attackers to cause a denial of service (application crash) via a crafted XML document.
CVE-2010-4033	Google Chrome before 7.0.517.41 does not properly implement the autofill and autocomplete functionality, which allows remote attackers to conduct "profile spamming" attacks via unspecified vectors.
CVE-2010-4034	Google Chrome before 7.0.517.41 does not properly handle forms, which allows remote attackers to cause

	a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.
CVE-2010-4035	Google Chrome before 7.0.517.41 does not properly perform autofill operations for forms, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.
CVE-2010-4036	Google Chrome before 7.0.517.41 does not properly handle the unloading of a page, which allows remote attackers to spoof URLs via unspecified vectors.
CVE-2010-4037	Unspecified vulnerability in Google Chrome before 7.0.517.41 allows remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2010-4038	The Web Sockets implementation in Google Chrome before 7.0.517.41 does not properly handle a shutdown action, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2010-4039	Google Chrome before 7.0.517.41 on Linux does not properly set the PATH environment variable, which has unspecified impact and attack vectors.
CVE-2010-4040	Google Chrome before 7.0.517.41 does not properly handle animated GIF images, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted image.
CVE-2010-4041	The sandbox implementation in Google Chrome before 7.0.517.41 on Linux does not properly constrain worker processes, which might allow remote attackers to bypass intended access restrictions via unspecified vectors.
CVE-2010-4042	Google Chrome before 7.0.517.41 does not properly handle element maps, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to "stale elements."
CVE-2010-4091	The EScript.api plugin in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.1, and 8.x before 8.2.6 on Windows and Mac OS X allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted PDF document that triggers memory corruption, involving the printSeps function. NOTE: some of these details are obtained from third party information.
CVE-2010-4197	Use-after-free vulnerability in WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving text editing.
CVE-2010-4198	WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, does

	not properly handle large text areas, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted HTML document.
CVE-2010-4199	Google Chrome before 7.0.517.44 does not properly perform a cast of an unspecified variable during processing of an SVG use element, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted SVG document.
CVE-2010-4201	Use-after-free vulnerability in Google Chrome before 7.0.517.44 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving text control selections.
CVE-2010-4202	Multiple integer overflows in Google Chrome before 7.0.517.44 on Linux allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted font.
CVE-2010-4203	WebM libvpx (aka the VP8 Codec SDK) before 0.9.5, as used in Google Chrome before 7.0.517.44, allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via invalid frames.
CVE-2010-4204	WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, accesses a frame object after this object has been destroyed, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2010-4205	Google Chrome before 7.0.517.44 does not properly handle the data types of event objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2010-4206	Array index error in the FEBlend::apply function in WebCore/platform/graphics/filters/FEBlend.cpp in WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a crafted SVG document, related to effects in the application of filters.
CVE-2010-4482	Unspecified vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2010-4483	Google Chrome before 8.0.552.215 does not properly restrict read access to videos derived from CANVAS elements, which allows remote attackers to bypass the Same Origin Policy and obtain potentially sensitive video data via a crafted web site.

CVE-2010-4484	Google Chrome before 8.0.552.215 does not properly handle HTML5 databases, which allows attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2010-4485	Google Chrome before 8.0.552.215 does not properly restrict the generation of file dialogs, which allows remote attackers to cause a denial of service (reduced usability and possible application crash) via a crafted web site.
CVE-2010-4486	Use-after-free vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to history handling.
CVE-2010-4487	Incomplete blacklist vulnerability in Google Chrome before 8.0.552.215 on Linux and Mac OS X allows remote attackers to have an unspecified impact via a "dangerous file."
CVE-2010-4488	Google Chrome before 8.0.552.215 does not properly handle HTTP proxy authentication, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2010-4489	libvpx, as used in Google Chrome before 8.0.552.215 and possibly other products, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WebM video. NOTE: this vulnerability exists because of a regression.
CVE-2010-4490	Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via malformed video content that triggers an indexing error.
CVE-2010-4491	Google Chrome before 8.0.552.215 does not properly restrict privileged extensions, which allows remote attackers to cause a denial of service (memory corruption) via a crafted extension.
CVE-2010-4492	Use-after-free vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG animations.
CVE-2010-4493	Use-after-free vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service via vectors related to the handling of mouse dragging events.
CVE-2010-4494	Double free vulnerability in libxml2 2.7.8 and other versions, as used in Google Chrome before 8.0.552.215 and other products, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XPath handling.

CVE-2010-4574	The Pickle::Pickle function in base/pickle.cc in Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 on 64-bit Linux platforms does not properly perform pointer arithmetic, which allows remote attackers to bypass message deserialization validation, and cause a denial of service or possibly have unspecified other impact, via invalid pickle data.
CVE-2010-4575	The ThemeInstalledInfoBarDelegate::Observe function in browser/extensions/ theme_installed_infobar_delegate.cc in Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 does not properly handle incorrect tab interaction by an extension, which allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted extension.
CVE-2010-4576	browser/worker_host/message_port_dispatcher.cc in Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 does not properly handle certain postMessage calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted JavaScript code that creates a web worker.
CVE-2010-4577	The CSSParser::parseFontFaceSrc function in WebCore/css/CSSParser.cpp in WebKit, as used in Google Chrome before 8.0.552.224, Chrome OS before 8.0.552.343, webkitgtk before 1.2.6, and other products does not properly parse Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted local font, related to "Type Confusion."
CVE-2010-4578	Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 do not properly perform cursor handling, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale pointers."
CVE-2010-4579	Opera before 11.00 does not properly constrain dialogs to appear on top of rendered documents, which makes it easier for remote attackers to trick users into interacting with a crafted web site that spoofs the (1) security information dialog or (2) download dialog.
CVE-2010-4580	Opera before 11.00 does not clear WAP WML form fields after manual navigation to a new web site, which allows remote attackers to obtain sensitive information via an input field that has the same name as an input field on a previously visited web site.
CVE-2010-4581	Unspecified vulnerability in Opera before 11.00 has unknown impact and attack vectors, related to "a high severity issue."
CVE-2010-4582	Opera before 11.00 does not properly handle security policies during updates to extensions, which might allow

	remote attackers to bypass intended access restrictions via unspecified vectors.
CVE-2010-4583	Opera before 11.00, when Opera Turbo is enabled, does not display a page's security indication, which makes it easier for remote attackers to spoof trusted content via a crafted web site.
CVE-2010-4584	Opera before 11.00, when Opera Turbo is used, does not properly present information about problematic X.509 certificates on https web sites, which might make it easier for remote attackers to spoof trusted content via a crafted web site.
CVE-2010-4585	Unspecified vulnerability in the auto-update functionality in Opera before 11.00 allows remote attackers to cause a denial of service (application crash) by triggering an Opera Unite update.
CVE-2010-4586	The default configuration of Opera before 11.00 enables WebSockets functionality, which has unspecified impact and remote attack vectors, possibly a related issue to CVE-2010-4508.
CVE-2010-4604	Stack-based buffer overflow in the GeneratePassword function in dsmtca (aka the Trusted Communications Agent or TCA) in the backup-archive client in IBM Tivoli Storage Manager (TSM) 5.3.x before 5.3.6.10, 5.4.x before 5.4.3.4, 5.5.x before 5.5.2.10, and 6.1.x before 6.1.3.1 on Unix and Linux allows local users to gain privileges by specifying a long LANG environment variable, and then sending a request over a pipe.
CVE-2010-4605	Unspecified vulnerability in the backup-archive client in IBM Tivoli Storage Manager (TSM) 5.3.x before 5.3.6.10, 5.4.x before 5.4.3.4, 5.5.x before 5.5.3, 6.1.x before 6.1.4, and 6.2.x before 6.2.2 on Unix and Linux allows local users to overwrite arbitrary files via unknown vectors.
CVE-2010-4606	Unspecified vulnerability in the Space Management client in the Hierarchical Storage Management (HSM) component in IBM Tivoli Storage Manager (TSM) 5.4.x before 5.4.3.4, 5.5.x before 5.5.3, 6.1.x before 6.1.4, and 6.2.x before 6.2.2 on Unix and Linux allows remote attackers to execute arbitrary commands via unknown vectors, related to a "script execution vulnerability."
CVE-2010-4785	The do_extendedOp function in ibmslapd in IBM Tivoli Directory Server (TDS) 6.0 before 6.0.0.62 (aka 6.0.0.8-TIV-ITDS-IF0004) on Linux, Solaris, and Windows allows remote authenticated users to cause a denial of service (ABEND) via a malformed LDAP extended operation that triggers certain comparisons involving the NULL operation OID.
CVE-2010-4786	IBM Tivoli Directory Server (TDS) 6.0 before 6.0.0.63 (aka 6.0.0.8-TIV-ITDS-IF0005) allows remote authenticated users to cause a denial of service

	(daemon crash or hang) via a paged search, as demonstrated by a certain idsldapsearch command, related to an improper ibm-slapdIdleTimeOut configuration setting.
CVE-2010-4787	IBM Tivoli Directory Server (TDS) 6.0 before 6.0.0.63 (aka 6.0.0.8-TIV-ITDS-IF0005) allows remote authenticated users to cause a denial of service (daemon hang) via a paged search that triggers improper mutex processing.
CVE-2010-4788	IBM Tivoli Directory Server (TDS) 6.0 before 6.0.0.62 (aka 6.0.0.8-TIV-ITDS-IF0004) does not perform certain locking of linked-list access, which allows remote authenticated users to cause a denial of service (daemon crash) via a paged search.
CVE-2010-4789	Use-after-free vulnerability in the proxy-server implementation in IBM Tivoli Directory Server (TDS) 6.0 before 6.0.0.65 (aka 6.0.0.8-TIV-ITDS-IF0007) and 6.3 before 6.3.0.1 (aka 6.3.0.0-TIV-ITDS-IF0001) allows remote authenticated users to cause a denial of service (daemon crash) via a paged search that is interrupted by an LDAP Unbind operation.
CVE-2011-0277	Cross-site request forgery (CSRF) vulnerability in HP Power Manager (HPPM) 4.3.2 and earlier allows remote attackers to hijack the authentication of administrators for requests that create new administrative accounts.
CVE-2011-0470	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle extensions notification, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2011-0471	The node-iteration implementation in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 does not properly handle pointers, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-0472	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle the printing of PDF documents, which allows user-assisted remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a multi-page document.
CVE-2011-0473	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle Cascading Style Sheets (CSS) token sequences in conjunction with CANVAS elements, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."

CVE-2011-0474	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle Cascading Style Sheets (CSS) token sequences in conjunction with cursors, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-0475	Use-after-free vulnerability in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a PDF document.
CVE-2011-0476	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 allow remote attackers to cause a denial of service (stack memory corruption) or possibly have unspecified other impact via a PDF document that triggers an out-of-memory error.
CVE-2011-0477	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle a mismatch in video frame sizes, which allows remote attackers to cause a denial of service (incorrect memory access) or possibly have unspecified other impact via unknown vectors.
CVE-2011-0478	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle SVG use elements, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-0479	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly interact with extensions, which allows remote attackers to cause a denial of service via a crafted extension that triggers an uninitialized pointer.
CVE-2011-0480	Multiple buffer overflows in vorbis_dec.c in the Vorbis decoder in FFmpeg, as used in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344, allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a crafted WebM file, related to buffers for (1) the channel floor and (2) the channel residue.
CVE-2011-0481	Buffer overflow in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to PDF shading.
CVE-2011-0482	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly perform a cast of an unspecified variable during handling of anchors, which

	allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted HTML document.
CVE-2011-0483	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly perform a cast of an unspecified variable during handling of video, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-0484	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly perform DOM node removal, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale rendering node."
CVE-2011-0485	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle speech data, which allows remote attackers to execute arbitrary code via unspecified vectors that lead to a "stale pointer."
CVE-2011-0558	Integer overflow in Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code via a large array length value in the ActionScript method of the Function class.
CVE-2011-0559	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted parameters to an unspecified ActionScript method that cause a parameter to be used as an object pointer, a different vulnerability than CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.
CVE-2011-0560	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.
CVE-2011-0561	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.
CVE-2011-0562	Untrusted search path vulnerability in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows allows local users to gain privileges via a Trojan horse DLL in the current working

	directory, a different vulnerability than CVE-2011-0570 and CVE-2011-0588.
CVE-2011-0563	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0589 and CVE-2011-0606.
CVE-2011-0565	Unspecified vulnerability in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-0585.
CVE-2011-0566	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted image, a different vulnerability than CVE-2011-0567 and CVE-2011-0603.
CVE-2011-0567	AcroRd32.dll in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted image that triggers an incorrect pointer calculation, leading to heap memory corruption, a different vulnerability than CVE-2011-0566 and CVE-2011-0603.
CVE-2011-0570	Untrusted search path vulnerability in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows allows local users to gain privileges via a Trojan horse DLL in the current working directory, a different vulnerability than CVE-2011-0562 and CVE-2011-0588.
CVE-2011-0571	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.
CVE-2011-0572	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.
CVE-2011-0573	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service

	(memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.
CVE-2011-0574	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.
CVE-2011-0575	Untrusted search path vulnerability in Adobe Flash Player before 10.2.152.26 allows local users to gain privileges via a Trojan horse DLL in the current working directory.
CVE-2011-0577	Unspecified vulnerability in Adobe Flash Player before 10.2.152.26 allows remote attackers to execute arbitrary code via a crafted font.
CVE-2011-0578	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors related to a constructor for an unspecified ActionScript3 object and improper type checking, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0607, and CVE-2011-0608.
CVE-2011-0579	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to obtain sensitive information via unspecified vectors.
CVE-2011-0585	Unspecified vulnerability in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-0565.
CVE-2011-0586	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X do not properly validate unspecified input data, which allows attackers to execute arbitrary code via unknown vectors.
CVE-2011-0587	Cross-site scripting (XSS) vulnerability in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2011-0604.

CVE-2011-0588	Untrusted search path vulnerability in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows allows local users to gain privileges via a Trojan horse DLL in the current working directory, a different vulnerability than CVE-2011-0562 and CVE-2011-0570.
CVE-2011-0589	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0563 and CVE-2011-0606.
CVE-2011-0590	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a 3D file, a different vulnerability than CVE-2011-0591, CVE-2011-0592, CVE-2011-0593, CVE-2011-0595, and CVE-2011-0600.
CVE-2011-0591	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a crafted Universal 3D (U3D) file that triggers a buffer overflow during decompression, related to Texture and rgba, a different vulnerability than CVE-2011-0590, CVE-2011-0592, CVE-2011-0593, CVE-2011-0595, and CVE-2011-0600.
CVE-2011-0592	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a crafted Universal 3D (U3D) file that triggers a buffer overflow during decompression, related to "Texture bmp," a different vulnerability than CVE-2011-0590, CVE-2011-0591, CVE-2011-0593, CVE-2011-0595, and CVE-2011-0600.
CVE-2011-0593	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a crafted Universal 3D (U3D) file that triggers a buffer overflow during decompression, a different vulnerability than CVE-2011-0590, CVE-2011-0591, CVE-2011-0592, CVE-2011-0595, and CVE-2011-0600.
CVE-2011-0594	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a font.
CVE-2011-0595	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a crafted Universal 3D (U3D) file

	that triggers a buffer overflow during decompression, a different vulnerability than CVE-2011-0590, CVE-2011-0591, CVE-2011-0592, CVE-2011-0593, and CVE-2011-0600.
CVE-2011-0596	The Bitmap parsing component in 2d.dll in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via an image with crafted (1) height and (2) width values for an RLE_8 compressed bitmap, which triggers a heap-based buffer overflow, a different vulnerability than CVE-2011-0598, CVE-2011-0599, and CVE-2011-0602.
CVE-2011-0598	Integer overflow in ACE.dll in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allows remote attackers to execute arbitrary code via crafted ICC data, a different vulnerability than CVE-2011-0596, CVE-2011-0599, and CVE-2011-0602.
CVE-2011-0599	The Bitmap parsing component in rt3d.dll in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a crafted image that causes an invalid pointer calculation related to 4/8-bit RLE compression, a different vulnerability than CVE-2011-0596, CVE-2011-0598, and CVE-2011-0602.
CVE-2011-0600	The U3D component in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a 3D file with an invalid Parent Node count that triggers an incorrect size calculation and memory corruption, a different vulnerability than CVE-2011-0590, CVE-2011-0591, CVE-2011-0592, CVE-2011-0593, and CVE-2011-0595.
CVE-2011-0602	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via crafted JP2K record types in a JPEG2000 image in a PDF file, which causes heap corruption, a different vulnerability than CVE-2011-0596, CVE-2011-0598, and CVE-2011-0599.
CVE-2011-0603	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted image, a different vulnerability than CVE-2011-0566 and CVE-2011-0567.
CVE-2011-0604	Cross-site scripting (XSS) vulnerability in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and

	8.x before 8.2.6 on Windows and Mac OS X allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2011-0587.
CVE-2011-0606	Stack-based buffer overflow in rt3d.dll in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors related to a crafted length value, a different vulnerability than CVE-2011-0563 and CVE-2011-0589.
CVE-2011-0607	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, and CVE-2011-0608.
CVE-2011-0608	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, and CVE-2011-0607.
CVE-2011-0609	Unspecified vulnerability in Adobe Flash Player 10.2.154.13 and earlier on Windows, Mac OS X, Linux, and Solaris; 10.1.106.16 and earlier on Android; Adobe AIR 2.5.1 and earlier; and Authplay.dll (aka AuthPlayLib.bundle) in Adobe Reader and Acrobat 9.x through 9.4.2 and 10.x through 10.0.1 on Windows and Mac OS X, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted Flash content, as demonstrated by a .swf file embedded in an Excel spreadsheet, and as exploited in the wild in March 2011.
CVE-2011-0611	Adobe Flash Player before 10.2.154.27 on Windows, Mac OS X, Linux, and Solaris and 10.2.156.12 and earlier on Android; Adobe AIR before 2.6.19140; and Authplay.dll (aka AuthPlayLib.bundle) in Adobe Reader 9.x before 9.4.4 and 10.x through 10.0.1 on Windows, Adobe Reader 9.x before 9.4.4 and 10.x before 10.0.3 on Mac OS X, and Adobe Acrobat 9.x before 9.4.4 and 10.x before 10.0.3 on Windows and Mac OS X allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted Flash content; as demonstrated by a Microsoft Office document with an embedded .swf file that has a size inconsistency in a "group of included constants," object type confusion, ActionScript that adds custom functions

	to prototypes, and Date objects; and as exploited in the wild in April 2011.
CVE-2011-0612	Adobe Flash Media Server (FMS) before 3.5.6, and 4.x before 4.0.2, allows remote attackers to cause a denial of service (XML data corruption) via unspecified vectors.
CVE-2011-0618	Integer overflow in Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-0619	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0620, CVE-2011-0621, and CVE-2011-0622.
CVE-2011-0620	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0619, CVE-2011-0621, and CVE-2011-0622.
CVE-2011-0621	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0619, CVE-2011-0620, and CVE-2011-0622.
CVE-2011-0622	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0619, CVE-2011-0620, and CVE-2011-0621.
CVE-2011-0623	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different vulnerability than CVE-2011-0624, CVE-2011-0625, and CVE-2011-0626.
CVE-2011-0624	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different vulnerability than CVE-2011-0623, CVE-2011-0625, and CVE-2011-0626.

CVE-2011-0625	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different vulnerability than CVE-2011-0623, CVE-2011-0624, and CVE-2011-0626.
CVE-2011-0626	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different vulnerability than CVE-2011-0623, CVE-2011-0624, and CVE-2011-0625.
CVE-2011-0627	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content, as possibly exploited in the wild in May 2011 by a Microsoft Office document with an embedded .swf file.
CVE-2011-0628	Integer overflow in Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows remote attackers to execute arbitrary code via ActionScript that improperly handles a long array object.
CVE-2011-0731	Buffer overflow in the DB2 Administration Server (DAS) component in IBM DB2 9.1 before FP10, 9.5 before FP7, and 9.7 before FP3 on Linux, UNIX, and Windows allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2011-0757	IBM DB2 9.1 before FP10, 9.5 before FP6a, and 9.7 before FP2 on Linux, UNIX, and Windows does not properly revoke the DBADM authority, which allows remote authenticated users to execute non-DDL statements by leveraging previous possession of this authority.
CVE-2011-0777	Use-after-free vulnerability in Google Chrome before 9.0.597.84 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to image loading.
CVE-2011-0778	Google Chrome before 9.0.597.84 does not properly restrict drag and drop operations, which might allow remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-0779	Google Chrome before 9.0.597.84 does not properly handle a missing key in an extension, which allows remote attackers to cause a denial of service (application crash) via a crafted extension.
CVE-2011-0780	The PDF event handler in Google Chrome before 9.0.597.84 does not properly interact with print operations, which allows user-assisted remote attackers

	to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-0781	Google Chrome before 9.0.597.84 does not properly handle autofill profile merging, which has unspecified impact and remote attack vectors.
CVE-2011-0783	Unspecified vulnerability in Google Chrome before 9.0.597.84 allows user-assisted remote attackers to cause a denial of service (application crash) via vectors involving a "bad volume setting."
CVE-2011-0784	Race condition in Google Chrome before 9.0.597.84 allows remote attackers to execute arbitrary code via vectors related to audio.
CVE-2011-0981	Google Chrome before 9.0.597.94 does not properly perform event handling for animations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-0982	Use-after-free vulnerability in Google Chrome before 9.0.597.94 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG font faces.
CVE-2011-0983	Google Chrome before 9.0.597.94 does not properly handle anonymous blocks, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-0984	Google Chrome before 9.0.597.94 does not properly handle plug-ins, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-0985	Google Chrome before 9.0.597.94 does not properly perform process termination upon memory exhaustion, which has unspecified impact and remote attack vectors.
CVE-2011-0994	Stack-based buffer overflow in NFRAgent.exe in Novell File Reporter (NFR) before 1.0.2 allows remote attackers to execute arbitrary code via unspecified XML data.
CVE-2011-1033	Stack-based buffer overflow in oninit in IBM Informix Dynamic Server (IDS) 11.50 allows remote attackers to execute arbitrary code via crafted arguments in the USELASTCOMMITTED session environment option in a SQL SET ENVIRONMENT statement.
CVE-2011-1038	Multiple cross-site scripting (XSS) vulnerabilities in stconf.nsf in the server in IBM Lotus Sametime 8.0.1 allow remote attackers to inject arbitrary web script or HTML via (1) the messageString parameter in a WebMessage action or (2) the PATH_INFO.

CVE-2011-1059	Use-after-free vulnerability in WebCore in WebKit before r77705, as used in Google Chrome before 11.0.672.2 and other products, allows user-assisted remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via vectors that entice a user to resubmit a form, related to improper handling of provisional items by the HistoryController component, aka rdar problem 8938557.
CVE-2011-1106	Cross-site scripting (XSS) vulnerability in stcenter.nsf in the server in IBM Lotus Sametime allows remote attackers to inject arbitrary web script or HTML via the authReasonCode parameter in an OpenDatabase action.
CVE-2011-1107	Unspecified vulnerability in Google Chrome before 9.0.597.107 allows remote attackers to spoof the URL bar via unknown vectors.
CVE-2011-1108	Google Chrome before 9.0.597.107 does not properly implement JavaScript dialogs, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.
CVE-2011-1109	Google Chrome before 9.0.597.107 does not properly process nodes in Cascading Style Sheets (CSS) stylesheets, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1110	Google Chrome before 9.0.597.107 does not properly implement key frame rules, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1111	Google Chrome before 9.0.597.107 does not properly implement forms controls, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1112	Google Chrome before 9.0.597.107 does not properly perform SVG rendering, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1113	Google Chrome before 9.0.597.107 on 64-bit Linux platforms does not properly perform pickle deserialization, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-1114	Google Chrome before 9.0.597.107 does not properly handle tables, which allows remote attackers to cause

	a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale node."
CVE-2011-1115	Google Chrome before 9.0.597.107 does not properly render tables, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1116	Google Chrome before 9.0.597.107 does not properly handle SVG animations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1117	Google Chrome before 9.0.597.107 does not properly handle XHTML documents, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale nodes."
CVE-2011-1118	Google Chrome before 9.0.597.107 does not properly handle TEXTAREA elements, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.
CVE-2011-1119	Google Chrome before 9.0.597.107 does not properly determine device orientation, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1120	The WebGL implementation in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors, aka Issue 71717.
CVE-2011-1121	Integer overflow in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a TEXTAREA element.
CVE-2011-1122	The WebGL implementation in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors, aka Issue 71960.
CVE-2011-1123	Google Chrome before 9.0.597.107 does not properly restrict access to internal extension functions, which has unspecified impact and remote attack vectors.
CVE-2011-1124	Use-after-free vulnerability in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to blocked plug-ins.
CVE-2011-1125	Google Chrome before 9.0.597.107 does not properly perform layout, which allows remote attackers to cause a denial of service or possibly have unspecified

	other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1185	Google Chrome before 10.0.648.127 does not prevent (1) navigation and (2) close operations on the top location of a sandboxed frame, which has unspecified impact and remote attack vectors.
CVE-2011-1186	Google Chrome before 10.0.648.127 on Linux does not properly handle parallel execution of calls to the print method, which might allow remote attackers to cause a denial of service (application crash) via crafted JavaScript code.
CVE-2011-1187	Google Chrome before 10.0.648.127 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, related to an "error message leak."
CVE-2011-1188	Google Chrome before 10.0.648.127 does not properly handle counter nodes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1189	Google Chrome before 10.0.648.127 does not properly perform box layout, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale node."
CVE-2011-1190	The Web Workers implementation in Google Chrome before 10.0.648.127 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, related to an "error message leak."
CVE-2011-1191	Use-after-free vulnerability in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of DOM URLs.
CVE-2011-1192	Google Chrome before 10.0.648.127 on Linux does not properly handle Unicode ranges, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-1193	Google V8, as used in Google Chrome before 10.0.648.127, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-1194	Multiple unspecified vulnerabilities in Google Chrome before 10.0.648.127 allow remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2011-1195	Use-after-free vulnerability in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to "document script lifetime handling."
CVE-2011-1196	The OGG container implementation in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other

	impact via unknown vectors that trigger an out-of-bounds write.
CVE-2011-1197	Google Chrome before 10.0.648.127 does not properly perform table painting, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1198	The video functionality in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger use of a malformed "out-of-bounds structure."
CVE-2011-1199	Google Chrome before 10.0.648.127 does not properly handle DataView objects, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1200	Google Chrome before 10.0.648.127 does not properly perform a cast of an unspecified variable during text rendering, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2011-1201	The context implementation in WebKit, as used in Google Chrome before 10.0.648.127, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1202	The xsltGenerateIdFunction function in functions.c in libxslt 1.1.26 and earlier, as used in Google Chrome before 10.0.648.127 and other products, allows remote attackers to obtain potentially sensitive information about heap memory addresses via an XML document containing a call to the XSLT generate-id XPath function.
CVE-2011-1203	Google Chrome before 10.0.648.127 does not properly handle SVG cursors, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1204	Google Chrome before 10.0.648.127 does not properly handle attributes, which allows remote attackers to cause a denial of service (DOM tree corruption) or possibly have unspecified other impact via a crafted document.
CVE-2011-1208	IBM solidDB 4.5.x before 4.5.182, 6.0.x before 6.0.1069, 6.1.x and 6.3.x before 6.3 FP8 (aka 6.3.49), and 6.5.x before 6.5 FP4 (aka 6.5.0.4) does not properly handle the (1) rpc_test_svc_readwrite and (2) rpc_test_svc_done commands, which allows remote attackers to cause a denial of service (NULL

	pointer dereference and daemon crash) via a crafted command.
CVE-2011-1285	The regular-expression functionality in Google Chrome before 10.0.648.127 does not properly implement reentrancy, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1286	Google V8, as used in Google Chrome before 10.0.648.127, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger incorrect access to memory.
CVE-2011-1290	Integer overflow in WebKit, as used on the Research In Motion (RIM) BlackBerry Torch 9800 with firmware 6.0.0.246, in Google Chrome before 10.0.648.133, and in Apple Safari before 5.0.5, allows remote attackers to execute arbitrary code via unknown vectors related to CSS "style handling," nodesets, and a length value, as demonstrated by Vincenzo Iozzo, Willem Pinckaers, and Ralf-Philipp Weinmann during a Pwn2Own competition at CanSecWest 2011.
CVE-2011-1291	Google Chrome before 10.0.648.204 does not properly handle base strings, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, related to a "buffer error."
CVE-2011-1292	Use-after-free vulnerability in the frame-loader implementation in Google Chrome before 10.0.648.204 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1293	Use-after-free vulnerability in the HTMLCollection implementation in Google Chrome before 10.0.648.204 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1294	Google Chrome before 10.0.648.204 does not properly handle Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1295	WebKit, as used in Google Chrome before 10.0.648.204 and Apple Safari before 5.0.6, does not properly handle node parentage, which allows remote attackers to cause a denial of service (DOM tree corruption), conduct cross-site scripting (XSS) attacks, or possibly have unspecified other impact via unknown vectors.

CVE-2011-1296	Google Chrome before 10.0.648.204 does not properly handle SVG text, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1301	Use-after-free vulnerability in the GPU process in Google Chrome before 10.0.648.205 allows remote attackers to execute arbitrary code via unknown vectors.
CVE-2011-1302	Heap-based buffer overflow in the GPU process in Google Chrome before 10.0.648.205 allows remote attackers to execute arbitrary code via unknown vectors.
CVE-2011-1303	Google Chrome before 11.0.696.57 does not properly handle floating objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1304	Unspecified vulnerability in Google Chrome before 11.0.696.57 allows remote attackers to bypass the pop-up blocker via vectors related to plug-ins.
CVE-2011-1305	Race condition in Google Chrome before 11.0.696.57 on Linux and Mac OS X allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to linked lists and a database.
CVE-2011-1360	Multiple cross-site scripting (XSS) vulnerabilities in IBM HTTP Server 2.0.47 and earlier, as used in WebSphere Application Server and other products, allow remote attackers to inject arbitrary web script or HTML via vectors involving unspecified documentation files in (1) manual/ibm/ and (2) htdocs/*/manual/ibm/.
CVE-2011-1393	Unspecified vulnerability in the authentication functionality in the server in IBM Lotus Domino 8.x before 8.5.2 FP4 allows remote attackers to cause a denial of service (daemon crash) via a crafted Notes RPC packet.
CVE-2011-1413	Google Chrome before 10.0.648.127 on Linux does not properly mitigate an unspecified flaw in an X server, which allows remote attackers to cause a denial of service (application crash) via vectors involving long messages.
CVE-2011-1434	Google Chrome before 11.0.696.57 does not ensure thread safety during handling of MIME data, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1435	Google Chrome before 11.0.696.57 does not properly implement the tabs permission for extensions, which

	allows remote attackers to read local files via a crafted extension.
CVE-2011-1436	Google Chrome before 11.0.696.57 on Linux does not properly interact with the X Window System, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2011-1437	Multiple integer overflows in Google Chrome before 11.0.696.57 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to float rendering.
CVE-2011-1438	Google Chrome before 11.0.696.57 allows remote attackers to bypass the Same Origin Policy via vectors involving blobs.
CVE-2011-1439	Google Chrome before 11.0.696.57 on Linux does not properly isolate renderer processes, which has unspecified impact and remote attack vectors.
CVE-2011-1440	Use-after-free vulnerability in Google Chrome before 11.0.696.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the ruby element and Cascading Style Sheets (CSS) token sequences.
CVE-2011-1441	Google Chrome before 11.0.696.57 does not properly perform a cast of an unspecified variable during handling of floating select lists, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted HTML document.
CVE-2011-1442	Google Chrome before 11.0.696.57 does not properly handle mutation events, which allows remote attackers to cause a denial of service (node tree corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1443	Google Chrome before 11.0.696.57 does not properly implement layering, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale pointers."
CVE-2011-1444	Race condition in the sandbox launcher implementation in Google Chrome before 11.0.696.57 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1445	Google Chrome before 11.0.696.57 does not properly handle SVG documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-1446	Google Chrome before 11.0.696.57 allows remote attackers to spoof the URL bar via vectors involving (1) a navigation error or (2) an interrupted load.

CVE-2011-1447	Google Chrome before 11.0.696.57 does not properly handle drop-down lists, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1448	Google Chrome before 11.0.696.57 does not properly perform height calculations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1449	Use-after-free vulnerability in the WebSockets implementation in Google Chrome before 11.0.696.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1450	Google Chrome before 11.0.696.57 does not properly present file dialogs, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "dangling pointers."
CVE-2011-1451	Google Chrome before 11.0.696.57 does not properly handle DOM id maps, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "dangling pointers."
CVE-2011-1452	Google Chrome before 11.0.696.57 allows user-assisted remote attackers to spoof the URL bar via vectors involving a redirect and a manual reload.
CVE-2011-1454	Use-after-free vulnerability in the DOM id handling functionality in Google Chrome before 11.0.696.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted HTML document.
CVE-2011-1455	Google Chrome before 11.0.696.57 does not properly handle PDF documents with multipart encoding, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.
CVE-2011-1456	Google Chrome before 11.0.696.57 does not properly handle PDF forms, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale pointers."
CVE-2011-1465	The SPDY implementation in net/http/http_network_transaction.cc in Google Chrome before 11.0.696.14 drains the bodies from SPDY responses, which might allow remote SPDY servers to cause a denial of service (application exit) by canceling a stream.

CVE-2011-1506	The STARTTLS implementation in Kerio Connect 7.1.4 build 2985 and MailServer 6.x does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a "plaintext command injection" attack, a similar issue to CVE-2011-0411. NOTE: some of these details are obtained from third party information.
CVE-2011-1540	Unspecified vulnerability in HP System Management Homepage (SMH) before 6.3 allows remote authenticated users to execute arbitrary code via unknown vectors.
CVE-2011-1541	Unspecified vulnerability in HP System Management Homepage (SMH) before 6.3 allows remote attackers to bypass intended access restrictions, and consequently execute arbitrary code, via unknown vectors.
CVE-2011-1542	Cross-site scripting (XSS) vulnerability in HP Systems Insight Manager (SIM) before 6.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2011-1543	Cross-site request forgery (CSRF) vulnerability in HP Systems Insight Manager (SIM) before 6.3 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.
CVE-2011-1560	solid.exe in IBM solidDB before 4.5.181, 6.0.x before 6.0.1067, 6.1.x and 6.3.x before 6.3.47, and 6.5.x before 6.5.0.3 uses a password-hash length specified by the client, which allows remote attackers to bypass authentication via a short length value.
CVE-2011-1691	The counterToCSSValue function in CSSComputedStyleDeclaration.cpp in the Cascading Style Sheets (CSS) implementation in WebCore in WebKit before r82222, as used in Google Chrome before 11.0.696.43 and other products, does not properly handle access to the (1) counterIncrement and (2) counterReset attributes of CSSStyleDeclaration data provided by a getComputedStyle method call, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted JavaScript code.
CVE-2011-1793	rendering/svg/RenderSVGResourceFilter.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted SVG document that leads to a "stale pointer."
CVE-2011-1794	Integer overflow in the FilterEffect::copyImageBytes function in platform/graphics/filters/FilterEffect.cpp in the SVG filter implementation in WebCore in WebKit

	in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted dimensions.
CVE-2011-1795	Integer underflow in the HTMLFormElement::removeFormElement function in html/HTMLFormElement.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document containing a FORM element.
CVE-2011-1796	Use-after-free vulnerability in the FrameView::calculateScrollbarModesForLayout function in page/FrameView.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code that calls the removeChild method during interaction with a FRAME element.
CVE-2011-1798	rendering/svg/RenderSVGText.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 does not properly perform a cast of an unspecified variable during an attempt to handle a block child, which allows remote attackers to cause a denial of service (application crash) or possibly have unknown other impact via a crafted text element in an SVG document.
CVE-2011-1799	Google Chrome before 11.0.696.68 does not properly perform casts of variables during interaction with the WebKit engine, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1800	Multiple integer overflows in the SVG Filters implementation in WebCore in WebKit in Google Chrome before 11.0.696.68 allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1801	Unspecified vulnerability in Google Chrome before 11.0.696.71 allows remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2011-1804	rendering/RenderBox.cpp in WebCore in WebKit before r86862, as used in Google Chrome before 11.0.696.71, does not properly render floats, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1806	Google Chrome before 11.0.696.71 does not properly implement the GPU command buffer, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

CVE-2011-1807	Google Chrome before 11.0.696.71 does not properly handle blobs, which allows remote attackers to execute arbitrary code via unspecified vectors that trigger an out-of-bounds write.
CVE-2011-1808	Use-after-free vulnerability in Google Chrome before 12.0.742.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to incorrect integer calculations during float handling.
CVE-2011-1809	Use-after-free vulnerability in the accessibility feature in Google Chrome before 12.0.742.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1810	The Cascading Style Sheets (CSS) implementation in Google Chrome before 12.0.742.91 does not properly restrict access to the visit history, which allows remote attackers to obtain sensitive information via unspecified vectors.
CVE-2011-1811	Google Chrome before 12.0.742.91 does not properly handle a large number of form submissions, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2011-1812	Google Chrome before 12.0.742.91 allows remote attackers to bypass intended access restrictions via vectors related to extensions.
CVE-2011-1813	Google Chrome before 12.0.742.91 does not properly implement the framework for extensions, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1814	Google Chrome before 12.0.742.91 attempts to read data from an uninitialized pointer, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1815	Google Chrome before 12.0.742.91 allows remote attackers to inject script into a tab page via vectors related to extensions.
CVE-2011-1816	Use-after-free vulnerability in the developer tools in Google Chrome before 12.0.742.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1817	Google Chrome before 12.0.742.91 does not properly implement history deletion, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1818	Use-after-free vulnerability in the image loader in Google Chrome before 12.0.742.91 allows remote

	attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1819	Google Chrome before 12.0.742.91 allows remote attackers to perform unspecified injection into a chrome:// page via vectors related to extensions.
CVE-2011-1846	IBM DB2 9.5 before FP7 and 9.7 before FP4 on Linux, UNIX, and Windows does not properly revoke role membership from groups, which allows remote authenticated users to execute non-DDL statements by leveraging previous inherited possession of a role, a different vulnerability than CVE-2011-0757. NOTE: some of these details are obtained from third party information.
CVE-2011-1847	IBM DB2 9.5 before FP7 and 9.7 before FP4 on Linux, UNIX, and Windows does not properly enforce privilege requirements for table access, which allows remote authenticated users to modify SYSSTAT.TABLES statistics columns via an UPDATE statement. NOTE: some of these details are obtained from third party information.
CVE-2011-2094	Buffer overflow in Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2095 and CVE-2011-2097.
CVE-2011-2095	Buffer overflow in Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2094 and CVE-2011-2097.
CVE-2011-2096	Heap-based buffer overflow in Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2097	Buffer overflow in Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2094 and CVE-2011-2095.
CVE-2011-2098	Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2099.
CVE-2011-2099	Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2098.

CVE-2011-2100	Untrusted search path vulnerability in Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows allows local users to gain privileges via a Trojan horse DLL in the current working directory.
CVE-2011-2101	Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X do not properly restrict script, which allows attackers to execute arbitrary code via a crafted document, related to a "cross document script execution vulnerability."
CVE-2011-2104	Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allow attackers to cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-2105	Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allow attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted font data.
CVE-2011-2107	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 10.3.181.22 on Windows, Mac OS X, Linux, and Solaris, and 10.3.185.22 and earlier on Android, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, related to a "universal cross-site scripting vulnerability."
CVE-2011-2110	Adobe Flash Player before 10.3.181.26 on Windows, Mac OS X, Linux, and Solaris, and 10.3.185.23 and earlier on Android, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as exploited in the wild in June 2011.
CVE-2011-2130	Buffer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2134, CVE-2011-2137, CVE-2011-2414, and CVE-2011-2415.
CVE-2011-2132	Adobe Flash Media Server (FMS) before 3.5.7, and 4.x before 4.0.3, allows attackers to cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-2134	Buffer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2130, CVE-2011-2137, CVE-2011-2414, and CVE-2011-2415.

CVE-2011-2135	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2140, CVE-2011-2417, and CVE-2011-2425.
CVE-2011-2136	Integer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2138 and CVE-2011-2416.
CVE-2011-2137	Buffer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2130, CVE-2011-2134, CVE-2011-2414, and CVE-2011-2415.
CVE-2011-2138	Integer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2136 and CVE-2011-2416.
CVE-2011-2139	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via unspecified vectors.
CVE-2011-2140	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2135, CVE-2011-2417, and CVE-2011-2425.
CVE-2011-2220	Stack-based buffer overflow in NFREngine.exe in Novell File Reporter Engine before 1.0.2.53, as used in Novell File Reporter and other products, allows remote attackers to execute arbitrary code via a crafted RECORD element.

CVE-2011-2332	Google V8, as used in Google Chrome before 12.0.742.91, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-2342	The DOM implementation in Google Chrome before 12.0.742.91 allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-2345	The NPAPI implementation in Google Chrome before 12.0.742.112 does not properly handle strings, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2346	Use-after-free vulnerability in Google Chrome before 12.0.742.112 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG fonts.
CVE-2011-2347	Google Chrome before 12.0.742.112 does not properly handle Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-2348	Google V8, as used in Google Chrome before 12.0.742.112, performs an incorrect bounds check, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2349	Use-after-free vulnerability in Google Chrome before 12.0.742.112 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to text selection.
CVE-2011-2350	The HTML parser in Google Chrome before 12.0.742.112 does not properly address "lifetime and re-entrancy issues," which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2351	Use-after-free vulnerability in Google Chrome before 12.0.742.112 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG use elements.
CVE-2011-2358	Google Chrome before 13.0.782.107 does not ensure that extension installations are confirmed by a browser dialog, which makes it easier for remote attackers to modify the product's functionality via a Trojan horse extension.
CVE-2011-2359	Google Chrome before 13.0.782.107 does not properly track line boxes during rendering, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-2360	Google Chrome before 13.0.782.107 does not ensure that the user is prompted before download of a

	dangerous file, which makes it easier for remote attackers to bypass intended content restrictions via a crafted web site.
CVE-2011-2361	The Basic Authentication dialog implementation in Google Chrome before 13.0.782.107 does not properly handle strings, which might make it easier for remote attackers to capture credentials via a crafted web site.
CVE-2011-2414	Buffer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2130, CVE-2011-2134, CVE-2011-2137, and CVE-2011-2415.
CVE-2011-2415	Buffer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2130, CVE-2011-2134, CVE-2011-2137, and CVE-2011-2414.
CVE-2011-2416	Integer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2136 and CVE-2011-2138.
CVE-2011-2417	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2135, CVE-2011-2140, and CVE-2011-2425.
CVE-2011-2424	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted SWF file, as demonstrated by "about 400 unique crash signatures."
CVE-2011-2425	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code or cause a

	denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2135, CVE-2011-2140, and CVE-2011-2417.
CVE-2011-2426	Stack-based buffer overflow in the ActionScript Virtual Machine (AVM) component in Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2427	Stack-based buffer overflow in the ActionScript Virtual Machine (AVM) component in Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows attackers to execute arbitrary code or cause a denial of service via unspecified vectors.
CVE-2011-2428	Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows attackers to execute arbitrary code or cause a denial of service (browser crash) via unspecified vectors, related to a "logic error issue."
CVE-2011-2429	Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, related to a "security control bypass."
CVE-2011-2430	Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows remote attackers to execute arbitrary code via crafted streaming media, related to a "logic error vulnerability."
CVE-2011-2431	Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allow attackers to execute arbitrary code via unspecified vectors, related to a "security bypass vulnerability."
CVE-2011-2432	Buffer overflow in the U3D TIFF Resource in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2433	Heap-based buffer overflow in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2434 and CVE-2011-2437.
CVE-2011-2434	Heap-based buffer overflow in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2433 and CVE-2011-2437.

CVE-2011-2435	Buffer overflow in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2436	Heap-based buffer overflow in the image-parsing library in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2437	Heap-based buffer overflow in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2433 and CVE-2011-2434.
CVE-2011-2438	Multiple stack-based buffer overflows in the image-parsing library in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allow attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2439	Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allow attackers to execute arbitrary code via unspecified vectors, related to a "memory leakage condition vulnerability."
CVE-2011-2440	Use-after-free vulnerability in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2441	Multiple stack-based buffer overflows in CoolType.dll in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allow attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2442	Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allow attackers to execute arbitrary code via unspecified vectors, related to a "logic error vulnerability."
CVE-2011-2444	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows remote attackers to inject arbitrary web script or HTML via a crafted URL, related to a "universal cross-site scripting issue," as exploited in the wild in September 2011.
CVE-2011-2445	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2451, CVE-2011-2452, CVE-2011-2453,

	CVE-2011-2454, CVE-2011-2455, CVE-2011-2459, and CVE-2011-2460.
CVE-2011-2450	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2011-2451	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2445, CVE-2011-2452, CVE-2011-2453, CVE-2011-2454, CVE-2011-2455, CVE-2011-2459, and CVE-2011-2460.
CVE-2011-2452	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2445, CVE-2011-2451, CVE-2011-2453, CVE-2011-2454, CVE-2011-2455, CVE-2011-2459, and CVE-2011-2460.
CVE-2011-2453	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2445, CVE-2011-2451, CVE-2011-2452, CVE-2011-2454, CVE-2011-2455, CVE-2011-2459, and CVE-2011-2460.
CVE-2011-2454	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2445, CVE-2011-2451, CVE-2011-2452, CVE-2011-2453, CVE-2011-2455, CVE-2011-2459, and CVE-2011-2460.
CVE-2011-2455	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2445, CVE-2011-2451, CVE-2011-2452,

	CVE-2011-2453, CVE-2011-2454, CVE-2011-2459, and CVE-2011-2460.
CVE-2011-2456	Buffer overflow in Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2457	Stack-based buffer overflow in Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2458	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, when Internet Explorer is used, allows remote attackers to bypass the cross-domain policy via a crafted web site.
CVE-2011-2459	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2445, CVE-2011-2451, CVE-2011-2452, CVE-2011-2453, CVE-2011-2454, CVE-2011-2455, and CVE-2011-2460.
CVE-2011-2460	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2445, CVE-2011-2451, CVE-2011-2452, CVE-2011-2453, CVE-2011-2454, CVE-2011-2455, and CVE-2011-2459.
CVE-2011-2462	Unspecified vulnerability in the U3D component in Adobe Reader and Acrobat 10.1.1 and earlier on Windows and Mac OS X, and Adobe Reader 9.x through 9.4.6 on UNIX, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, as exploited in the wild in December 2011.
CVE-2011-2463	Cross-site scripting (XSS) vulnerability in Adobe ColdFusion 8.0 through 9.0.1 allows remote attackers to inject arbitrary web script or HTML via vectors involving the cfform tag.

CVE-2011-2474	Directory traversal vulnerability in the HTTP Server in Sybase EAServer 6.3.1 Developer Edition allows remote attackers to read arbitrary files via a /.\../\../\ sequence in a path.
CVE-2011-2750	NFRAgent.exe in Novell File Reporter 1.0.4.2 and earlier allows remote attackers to delete arbitrary files via a full pathname in an SRS OPERATION 4 CMD 5 request to /FSF/CMD.
CVE-2011-2758	IDSWebApp in the Web Administration Tool in IBM Tivoli Directory Server (TDS) 6.2 before 6.2.0.3-TIV-ITDS-IF0004 does not require authentication for access to LDAP Server log files, which allows remote attackers to obtain sensitive information via a crafted URL.
CVE-2011-2759	The login page of IDSWebApp in the Web Administration Tool in IBM Tivoli Directory Server (TDS) 6.2 before 6.2.0.3-TIV-ITDS-IF0004 does not have an off autocomplete attribute for authentication fields, which makes it easier for remote attackers to obtain access by leveraging an unattended workstation.
CVE-2011-2761	Google Chrome 14.0.794.0 does not properly handle a reload of a page generated in response to a POST, which allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted web site, related to GetWidget methods.
CVE-2011-2782	The drag-and-drop implementation in Google Chrome before 13.0.782.107 on Linux does not properly enforce permissions for files, which allows user-assisted remote attackers to bypass intended access restrictions via unspecified vectors.
CVE-2011-2783	Google Chrome before 13.0.782.107 does not ensure that developer-mode NPAPI extension installations are confirmed by a browser dialog, which makes it easier for remote attackers to modify the product's functionality via a Trojan horse extension.
CVE-2011-2784	Google Chrome before 13.0.782.107 allows remote attackers to obtain sensitive information via a request for the GL program log, which reveals a local path in an unspecified log entry.
CVE-2011-2785	The extensions implementation in Google Chrome before 13.0.782.107 does not properly validate the URL for the home page, which allows remote attackers to have an unspecified impact via a crafted extension.
CVE-2011-2786	Google Chrome before 13.0.782.107 does not ensure that the speech-input bubble is shown on the product's screen, which might make it easier for remote attackers to make audio recordings via a crafted web page containing an INPUT element.
CVE-2011-2787	Google Chrome before 13.0.782.107 does not properly address re-entrancy issues associated with the GPU

	lock, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2011-2788	Buffer overflow in the inspector serialization functionality in Google Chrome before 13.0.782.107 allows user-assisted remote attackers to have an unspecified impact via unknown vectors.
CVE-2011-2789	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to instantiation of the Pepper plug-in.
CVE-2011-2790	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving floating styles.
CVE-2011-2791	The International Components for Unicode (ICU) functionality in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.
CVE-2011-2792	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to float removal.
CVE-2011-2793	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to media selectors.
CVE-2011-2794	Google Chrome before 13.0.782.107 does not properly perform text iteration, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2795	Google Chrome before 13.0.782.107 does not prevent calls to functions in other frames, which allows remote attackers to bypass intended access restrictions via a crafted web site, related to a "cross-frame function leak."
CVE-2011-2796	Use-after-free vulnerability in Skia, as used in Google Chrome before 13.0.782.107, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2797	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to resource caching.
CVE-2011-2798	Google Chrome before 13.0.782.107 does not properly restrict access to internal schemes, which allows remote attackers to have an unspecified impact via a crafted web site.

CVE-2011-2799	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to HTML range handling.
CVE-2011-2800	Google Chrome before 13.0.782.107 allows remote attackers to obtain potentially sensitive information about client-side redirect targets via a crafted web site.
CVE-2011-2801	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the frame loader.
CVE-2011-2802	Google V8, as used in Google Chrome before 13.0.782.107, does not properly perform const lookups, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted web site.
CVE-2011-2803	Google Chrome before 13.0.782.107 does not properly handle Skia paths, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2804	Google Chrome before 13.0.782.107 does not properly handle nested functions in PDF documents, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted document.
CVE-2011-2805	Google Chrome before 13.0.782.107 allows remote attackers to bypass the Same Origin Policy and conduct script injection attacks via unspecified vectors.
CVE-2011-2818	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to display box rendering.
CVE-2011-2819	Google Chrome before 13.0.782.107 allows remote attackers to bypass the Same Origin Policy via vectors related to handling of the base URI.
CVE-2011-2821	Double free vulnerability in libxml2, as used in Google Chrome before 13.0.782.215, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted XPath expression.
CVE-2011-2823	Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a line box.
CVE-2011-2824	Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving counter nodes.

CVE-2011-2825	Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving custom fonts.
CVE-2011-2826	Google Chrome before 13.0.782.215 allows remote attackers to bypass the Same Origin Policy via vectors related to empty origins.
CVE-2011-2827	Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to text searching.
CVE-2011-2828	Google V8, as used in Google Chrome before 13.0.782.215, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.
CVE-2011-2829	Integer overflow in Google Chrome before 13.0.782.215 on 32-bit platforms allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving uniform arrays.
CVE-2011-2830	Google V8, as used in Google Chrome before 14.0.835.163, does not properly implement script object wrappers, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-2834	Double free vulnerability in libxml2, as used in Google Chrome before 14.0.835.163, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XPath handling.
CVE-2011-2835	Race condition in Google Chrome before 14.0.835.163 allows attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the certificate cache.
CVE-2011-2836	Google Chrome before 14.0.835.163 does not require Infobar interaction before use of the Windows Media Player plug-in, which makes it easier for remote attackers to have an unspecified impact via crafted Flash content.
CVE-2011-2837	Google Chrome before 14.0.835.163 on Linux does not use the PIC and PIE compiler options for position-independent code, which has unspecified impact and attack vectors.
CVE-2011-2838	Google Chrome before 14.0.835.163 does not properly consider the MIME type during the loading of a plug-in, which has unspecified impact and remote attack vectors.
CVE-2011-2839	The PDF implementation in Google Chrome before 13.0.782.215 on Linux does not properly use the memset library function, which allows remote

	attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2840	Google Chrome before 14.0.835.163 allows user-assisted remote attackers to spoof the URL bar via vectors related to "unusual user interaction."
CVE-2011-2841	Google Chrome before 14.0.835.163 does not properly perform garbage collection during the processing of PDF documents, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2011-2843	Google Chrome before 14.0.835.163 does not properly handle media buffers, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2844	Google Chrome before 14.0.835.163 does not properly process MP3 files, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2845	Google Chrome before 15.0.874.102 does not properly handle history data, which allows user-assisted remote attackers to spoof the URL bar via unspecified vectors.
CVE-2011-2846	Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to unload event handling.
CVE-2011-2847	Use-after-free vulnerability in the document loader in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2011-2848	Google Chrome before 14.0.835.163 allows user-assisted remote attackers to spoof the URL bar via vectors related to the forward button.
CVE-2011-2849	The WebSockets implementation in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via unspecified vectors.
CVE-2011-2850	Google Chrome before 14.0.835.163 does not properly handle Khmer characters, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2851	Google Chrome before 14.0.835.163 does not properly handle video, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2852	Off-by-one error in Google V8, as used in Google Chrome before 14.0.835.163, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

CVE-2011-2853	Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to plug-in handling.
CVE-2011-2854	Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to "ruby / table style handing."
CVE-2011-2855	Google Chrome before 14.0.835.163 does not properly handle Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale node."
CVE-2011-2856	Google V8, as used in Google Chrome before 14.0.835.163, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-2857	Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the focus controller.
CVE-2011-2858	Google Chrome before 14.0.835.163 does not properly handle triangle arrays, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2859	Google Chrome before 14.0.835.163 uses incorrect permissions for non-gallery pages, which has unspecified impact and attack vectors.
CVE-2011-2860	Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to table styles.
CVE-2011-2861	Google Chrome before 14.0.835.163 does not properly handle strings in PDF documents, which allows remote attackers to have an unspecified impact via a crafted document that triggers an incorrect read operation.
CVE-2011-2862	Google V8, as used in Google Chrome before 14.0.835.163, does not properly restrict access to built-in objects, which has unspecified impact and remote attack vectors.
CVE-2011-2864	Google Chrome before 14.0.835.163 does not properly handle Tibetan characters, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2874	Google Chrome before 14.0.835.163 does not perform an expected pin operation for a self-signed certificate during a session, which has unspecified impact and remote attack vectors.
CVE-2011-2875	Google V8, as used in Google Chrome before 14.0.835.163, does not properly perform object sealing,

	which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2011-2876	Use-after-free vulnerability in Google Chrome before 14.0.835.202 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a text line box.
CVE-2011-2877	Google Chrome before 14.0.835.202 does not properly handle SVG text, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale font."
CVE-2011-2878	Google Chrome before 14.0.835.202 does not properly restrict access to the window prototype, which allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-2879	Google Chrome before 14.0.835.202 does not properly consider object lifetimes and thread safety during the handling of audio nodes, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2880	Use-after-free vulnerability in Google Chrome before 14.0.835.202 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the Google V8 bindings.
CVE-2011-2881	Google Chrome before 14.0.835.202 does not properly handle Google V8 hidden objects, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2011-2903	Heap-based buffer overflow in tcptrack before 1.4.2 might allow attackers to execute arbitrary code via a long command line argument. NOTE: this is only a vulnerability in limited scenarios in which tcptrack is "configured as a handler for other applications." This issue might not qualify for inclusion in CVE.
CVE-2011-3015	Multiple integer overflows in the PDF codecs in Google Chrome before 17.0.963.56 allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3016	Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving counter nodes, related to a "read-after-free" issue.
CVE-2011-3017	Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to database handling.

CVE-2011-3018	Heap-based buffer overflow in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to path rendering.
CVE-2011-3019	Heap-based buffer overflow in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Matroska video (aka MKV) file.
CVE-2011-3020	Unspecified vulnerability in the Native Client validator implementation in Google Chrome before 17.0.963.56 has unknown impact and remote attack vectors.
CVE-2011-3021	Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to subframe loading.
CVE-2011-3022	translate/translate_manager.cc in Google Chrome before 17.0.963.56 and 19.x before 19.0.1036.7 uses an HTTP session to exchange data for translation, which allows remote attackers to obtain sensitive information by sniffing the network.
CVE-2011-3023	Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to drag-and-drop operations.
CVE-2011-3024	Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service (application crash) via an empty X.509 certificate.
CVE-2011-3025	Google Chrome before 17.0.963.56 does not properly parse H.264 data, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3026	Integer overflow in libpng, as used in Google Chrome before 17.0.963.56, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an integer truncation.
CVE-2011-3027	Google Chrome before 17.0.963.56 does not properly perform a cast of an unspecified variable during handling of columns, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2011-3031	Use-after-free vulnerability in the element wrapper in Google V8, as used in Google Chrome before 17.0.963.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3032	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial

	of service or possibly have unspecified other impact via vectors related to the handling of SVG values.
CVE-2011-3033	Buffer overflow in Skia, as used in Google Chrome before 17.0.963.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3034	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving an SVG document.
CVE-2011-3035	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG use elements.
CVE-2011-3036	Google Chrome before 17.0.963.65 does not properly perform a cast of an unspecified variable during handling of line boxes, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2011-3037	Google Chrome before 17.0.963.65 does not properly perform casts of unspecified variables during the splitting of anonymous blocks, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2011-3038	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to multi-column handling.
CVE-2011-3039	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to quote handling.
CVE-2011-3040	Google Chrome before 17.0.963.65 does not properly handle text, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.
CVE-2011-3041	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of class attributes.
CVE-2011-3042	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of table sections.
CVE-2011-3043	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a flexbox (aka flexible box) in conjunction with the floating of elements.

CVE-2011-3044	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG animation elements.
CVE-2011-3045	Integer signedness error in the png_inflate function in pngrutil.c in libpng before 1.4.10beta01, as used in Google Chrome before 17.0.963.83 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PNG file, a different vulnerability than CVE-2011-3026.
CVE-2011-3046	The extension subsystem in Google Chrome before 17.0.963.78 does not properly handle history navigation, which allows remote attackers to execute arbitrary code by leveraging a "Universal XSS (UXSS)" issue.
CVE-2011-3047	The GPU process in Google Chrome before 17.0.963.79 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) by leveraging an error in the plug-in loading mechanism.
CVE-2011-3049	Google Chrome before 17.0.963.83 does not properly restrict the extension web request API, which allows remote attackers to cause a denial of service (disrupted system requests) via a crafted extension.
CVE-2011-3050	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 17.0.963.83 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the :first-letter pseudo-element.
CVE-2011-3051	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 17.0.963.83 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the cross-fade function.
CVE-2011-3052	The WebGL implementation in Google Chrome before 17.0.963.83 does not properly handle CANVAS elements, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-3053	Use-after-free vulnerability in Google Chrome before 17.0.963.83 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to block splitting.
CVE-2011-3054	The WebUI privilege implementation in Google Chrome before 17.0.963.83 does not properly perform isolation, which allows remote attackers to bypass intended access restrictions via unspecified vectors.

CVE-2011-3055	The browser native UI in Google Chrome before 17.0.963.83 does not require user confirmation before an unpacked extension installation, which allows user-assisted remote attackers to have an unspecified impact via a crafted extension.
CVE-2011-3056	Google Chrome before 17.0.963.83 allows remote attackers to bypass the Same Origin Policy via vectors involving a "magic iframe."
CVE-2011-3057	Google V8, as used in Google Chrome before 17.0.963.83, allows remote attackers to cause a denial of service via vectors that trigger an invalid read operation.
CVE-2011-3058	Google Chrome before 18.0.1025.142 does not properly handle the EUC-JP encoding system, which might allow remote attackers to conduct cross-site scripting (XSS) attacks via unspecified vectors.
CVE-2011-3059	Google Chrome before 18.0.1025.142 does not properly handle SVG text elements, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3060	Google Chrome before 18.0.1025.142 does not properly handle text fragments, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3061	Google Chrome before 18.0.1025.142 does not properly check X.509 certificates before use of a SPDY proxy, which might allow man-in-the-middle attackers to spoof servers or obtain sensitive information via a crafted certificate.
CVE-2011-3062	Off-by-one error in the OpenType Sanitizer in Google Chrome before 18.0.1025.142 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted OpenType file.
CVE-2011-3063	Google Chrome before 18.0.1025.142 does not properly validate the renderer's navigation requests, which has unspecified impact and remote attack vectors.
CVE-2011-3064	Use-after-free vulnerability in Google Chrome before 18.0.1025.142 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG clipping.
CVE-2011-3065	Skia, as used in Google Chrome before 18.0.1025.142, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-3066	Skia, as used in Google Chrome before 18.0.1025.151, does not properly perform clipping, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.

CVE-2011-3067	Google Chrome before 18.0.1025.151 allows remote attackers to bypass the Same Origin Policy via vectors related to replacement of IFRAME elements.
CVE-2011-3068	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to run-in boxes.
CVE-2011-3069	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to line boxes.
CVE-2011-3070	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the Google V8 bindings.
CVE-2011-3071	Use-after-free vulnerability in the HTMLMediaElement implementation in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3072	Google Chrome before 18.0.1025.151 allows remote attackers to bypass the Same Origin Policy via vectors related to pop-up windows.
CVE-2011-3073	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of SVG resources.
CVE-2011-3074	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of media.
CVE-2011-3075	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to style-application commands.
CVE-2011-3076	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to focus handling.
CVE-2011-3077	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the script bindings, related to a "read-after-free" issue.

CVE-2011-3078	Use-after-free vulnerability in Google Chrome before 18.0.1025.168 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the floating of elements, a different vulnerability than CVE-2011-3081.
CVE-2011-3079	The Inter-process Communication (IPC) implementation in Google Chrome before 18.0.1025.168, as used in Mozilla Firefox before 38.0 and other products, does not properly validate messages, which has unspecified impact and attack vectors.
CVE-2011-3080	Race condition in the Inter-process Communication (IPC) implementation in Google Chrome before 18.0.1025.168 allows attackers to bypass intended sandbox restrictions via unspecified vectors.
CVE-2011-3081	Use-after-free vulnerability in Google Chrome before 18.0.1025.168 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the floating of elements, a different vulnerability than CVE-2011-3078.
CVE-2011-3083	browser/profiles/profile_impl_io_data.cc in Google Chrome before 19.0.1084.46 does not properly handle a malformed ftp URL in the SRC attribute of a VIDEO element, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted web page.
CVE-2011-3084	Google Chrome before 19.0.1084.46 does not use a dedicated process for the loading of links found on an internal page, which might allow attackers to bypass intended sandbox restrictions via a crafted page.
CVE-2011-3085	The Autofill feature in Google Chrome before 19.0.1084.46 does not properly restrict field values, which allows remote attackers to cause a denial of service (UI corruption) and possibly conduct spoofing attacks via vectors involving long values.
CVE-2011-3086	Use-after-free vulnerability in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a STYLE element.
CVE-2011-3087	Google Chrome before 19.0.1084.46 does not properly perform window navigation, which has unspecified impact and remote attack vectors.
CVE-2011-3088	Google Chrome before 19.0.1084.46 does not properly draw hairlines, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3089	Use-after-free vulnerability in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving tables.

CVE-2011-3090	Race condition in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to worker processes.
CVE-2011-3091	Use-after-free vulnerability in the IndexedDB implementation in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3092	The regex implementation in Google V8, as used in Google Chrome before 19.0.1084.46, allows remote attackers to cause a denial of service (invalid write operation) or possibly have unspecified other impact via unknown vectors.
CVE-2011-3093	Google Chrome before 19.0.1084.46 does not properly handle glyphs, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3094	Google Chrome before 19.0.1084.46 does not properly handle Tibetan text, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3095	The OGG container in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.
CVE-2011-3096	Use-after-free vulnerability in Google Chrome before 19.0.1084.46 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging an error in the GTK implementation of the omnibox.
CVE-2011-3097	The PDF functionality in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging an out-of-bounds write error in the implementation of sampled functions.
CVE-2011-3099	Use-after-free vulnerability in the PDF functionality in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a malformed name for the font encoding.
CVE-2011-3100	Google Chrome before 19.0.1084.46 does not properly draw dash paths, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3101	Google Chrome before 19.0.1084.46 on Linux does not properly mitigate an unspecified flaw in an NVIDIA driver, which has unknown impact and attack vectors.

	NOTE: see CVE-2012-3105 for the related MFSA 2012-34 issue in Mozilla products.
CVE-2011-3102	Off-by-one error in libxml2, as used in Google Chrome before 19.0.1084.46 and other products, allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via unknown vectors.
CVE-2011-3103	Google V8, as used in Google Chrome before 19.0.1084.52, does not properly perform garbage collection, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2011-3104	Skia, as used in Google Chrome before 19.0.1084.52, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3105	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 19.0.1084.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the :first-letter pseudo-element.
CVE-2011-3106	The WebSockets implementation in Google Chrome before 19.0.1084.52 does not properly handle use of SSL, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-3107	Google Chrome before 19.0.1084.52 does not properly implement JavaScript bindings for plug-ins, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-3108	Use-after-free vulnerability in Google Chrome before 19.0.1084.52 allows remote attackers to execute arbitrary code via vectors related to the browser cache.
CVE-2011-3109	Google Chrome before 19.0.1084.52 on Linux does not properly perform a cast of an unspecified variable, which allows remote attackers to cause a denial of service or possibly have unknown other impact by leveraging an error in the GTK implementation of the UI.
CVE-2011-3110	The PDF functionality in Google Chrome before 19.0.1084.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.
CVE-2011-3111	Google V8, as used in Google Chrome before 19.0.1084.52, allows remote attackers to cause a denial of service (invalid read operation) via unspecified vectors.
CVE-2011-3112	Use-after-free vulnerability in the PDF functionality in Google Chrome before 19.0.1084.52 allows remote

	attackers to cause a denial of service or possibly have unspecified other impact via an invalid encrypted document.
CVE-2011-3113	The PDF functionality in Google Chrome before 19.0.1084.52 does not properly perform a cast of an unspecified variable during handling of color spaces, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2011-3114	Multiple buffer overflows in the PDF functionality in Google Chrome before 19.0.1084.52 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger unknown function calls.
CVE-2011-3115	Google V8, as used in Google Chrome before 19.0.1084.52, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger "type corruption."
CVE-2011-3234	Google Chrome before 14.0.835.163 does not properly handle boxes, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3388	Opera before 11.51 allows remote attackers to cause an insecure site to appear secure or trusted via unspecified actions related to Extended Validation and loading content from trusted sources in an unspecified sequence that causes the address field and page information dialog to contain security information based on the trusted site, instead of the insecure site.
CVE-2011-3389	The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.
CVE-2011-3390	Multiple cross-site scripting (XSS) vulnerabilities in index.php in IBM OpenAdmin Tool (OAT) before 2.72 for Informix allow remote attackers to inject arbitrary web script or HTML via the (1) informixserver, (2) host, or (3) port parameter in a login action.
CVE-2011-3846	Cross-site request forgery (CSRF) vulnerability in HP System Management Homepage (SMH) 6.2.2.7 allows remote attackers to hijack the authentication of administrators for requests that create administrative accounts.

CVE-2011-3873	Google Chrome before 14.0.835.202 does not properly implement shader translation, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-3875	Google Chrome before 15.0.874.102 does not properly handle drag and drop operations on URL strings, which allows user-assisted remote attackers to spoof the URL bar via unspecified vectors.
CVE-2011-3876	Google Chrome before 15.0.874.102 does not properly handle downloading files that have whitespace characters at the end of a filename, which has unspecified impact and user-assisted remote attack vectors.
CVE-2011-3877	Cross-site scripting (XSS) vulnerability in the appcache internals page in Google Chrome before 15.0.874.102 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2011-3878	Race condition in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to worker process initialization.
CVE-2011-3879	Google Chrome before 15.0.874.102 does not prevent redirects to chrome: URLs, which has unspecified impact and remote attack vectors.
CVE-2011-3880	Google Chrome before 15.0.874.102 does not prevent use of an unspecified special character as a delimiter in HTTP headers, which has unknown impact and remote attack vectors.
CVE-2011-3881	WebKit, as used in Google Chrome before 15.0.874.102 and Android before 4.4, allows remote attackers to bypass the Same Origin Policy and conduct Universal XSS (UXSS) attacks via vectors related to (1) the DOMWindow::clear function and use of a selection object, (2) the Object::GetRealNamedPropertyInPrototypeChain function and use of an __proto__ property, (3) the HTMLPlugInImageElement::allowedToLoadFrameURL function and use of a javascript: URL, (4) incorrect origins for XSLT-generated documents in the XSLTProcessor::createDocumentFromSource function, and (5) improper handling of synchronous frame loads in the ScriptController::executeIfJavaScriptURL function.
CVE-2011-3882	Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to media buffers.
CVE-2011-3883	Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial

	of service or possibly have unspecified other impact via vectors related to counters.
CVE-2011-3884	Google Chrome before 15.0.874.102 does not properly address timing issues during DOM traversal, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2011-3885	Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to stale Cascading Style Sheets (CSS) token-sequence data.
CVE-2011-3886	Google V8, as used in Google Chrome before 15.0.874.102, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers out-of-bounds write operations.
CVE-2011-3887	Google Chrome before 15.0.874.102 does not properly handle javascript: URLs, which allows remote attackers to bypass intended access restrictions and read cookies via unspecified vectors.
CVE-2011-3888	Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to editing operations in conjunction with an unknown plug-in.
CVE-2011-3889	Heap-based buffer overflow in the Web Audio implementation in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3890	Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to video source handling.
CVE-2011-3891	Google Chrome before 15.0.874.102 does not properly restrict access to internal Google V8 functions, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3892	Double free vulnerability in the Theora decoder in Google Chrome before 15.0.874.120 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted stream.
CVE-2011-3893	Google Chrome before 15.0.874.120 does not properly implement the MKV and Vorbis media handlers, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.

CVE-2011-3894	Google Chrome before 15.0.874.120 does not properly perform VP8 decoding, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted stream.
CVE-2011-3895	Heap-based buffer overflow in the Vorbis decoder in Google Chrome before 15.0.874.120 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted stream.
CVE-2011-3896	Buffer overflow in Google Chrome before 15.0.874.120 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to shader variable mapping.
CVE-2011-3897	Use-after-free vulnerability in Google Chrome before 15.0.874.120 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to editing.
CVE-2011-3898	Google Chrome before 15.0.874.120, when Java Runtime Environment (JRE) 7 is used, does not request user confirmation before applet execution begins, which allows remote attackers to have an unspecified impact via a crafted applet.
CVE-2011-3900	Google V8, as used in Google Chrome before 15.0.874.121, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write operation.
CVE-2011-3903	Google Chrome before 16.0.912.63 does not properly perform regex matching, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3904	Use-after-free vulnerability in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to bidirectional text (aka bidi) handling.
CVE-2011-3905	libxml2, as used in Google Chrome before 16.0.912.63, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3906	The PDF parser in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3907	The view-source feature in Google Chrome before 16.0.912.63 allows remote attackers to spoof the URL bar via unspecified vectors.
CVE-2011-3908	Google Chrome before 16.0.912.63 does not properly parse SVG documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.

CVE-2011-3909	The Cascading Style Sheets (CSS) implementation in Google Chrome before 16.0.912.63 on 64-bit platforms does not properly manage property arrays, which allows remote attackers to cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-3910	Google Chrome before 16.0.912.63 does not properly handle YUV video frames, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3911	Google Chrome before 16.0.912.63 does not properly handle PDF documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3912	Use-after-free vulnerability in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG filters.
CVE-2011-3913	Use-after-free vulnerability in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to Range handling.
CVE-2011-3914	The internationalization (aka i18n) functionality in Google V8, as used in Google Chrome before 16.0.912.63, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.
CVE-2011-3915	Buffer overflow in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to PDF fonts.
CVE-2011-3916	Google Chrome before 16.0.912.63 does not properly handle PDF cross references, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3917	Stack-based buffer overflow in FileWatcher in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3919	Heap-based buffer overflow in libxml2, as used in Google Chrome before 16.0.912.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3921	Use-after-free vulnerability in Google Chrome before 16.0.912.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving animation frames.
CVE-2011-3922	Stack-based buffer overflow in Google Chrome before 16.0.912.75 allows remote attackers to cause a denial

	of service or possibly have unspecified other impact via vectors related to glyph handling.
CVE-2011-3924	Use-after-free vulnerability in Google Chrome before 16.0.912.77 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOM selections.
CVE-2011-3925	Use-after-free vulnerability in the Safe Browsing feature in Google Chrome before 16.0.912.75 allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via vectors related to a navigation entry and an interstitial page.
CVE-2011-3926	Heap-based buffer overflow in the tree builder in Google Chrome before 16.0.912.77 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3927	Skia, as used in Google Chrome before 16.0.912.77, does not perform all required initialization of values, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3928	Use-after-free vulnerability in Google Chrome before 16.0.912.77 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOM handling.
CVE-2011-3953	Google Chrome before 17.0.963.46 does not prevent monitoring of the clipboard after a paste event, which has unspecified impact and remote attack vectors.
CVE-2011-3954	Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (application crash) via vectors that trigger a large amount of database usage.
CVE-2011-3955	Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via vectors that trigger the aborting of an IndexedDB transaction.
CVE-2011-3956	The extension implementation in Google Chrome before 17.0.963.46 does not properly handle sandboxed origins, which might allow remote attackers to bypass the Same Origin Policy via a crafted extension.
CVE-2011-3957	Use-after-free vulnerability in the garbage-collection functionality in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving PDF documents.
CVE-2011-3958	Google Chrome before 17.0.963.46 does not properly perform casts of variables during handling of a column

	span, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2011-3959	Buffer overflow in the locale implementation in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3960	Google Chrome before 17.0.963.46 does not properly decode audio data, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3961	Race condition in Google Chrome before 17.0.963.46 allows remote attackers to execute arbitrary code via vectors that trigger a crash of a utility process.
CVE-2011-3962	Google Chrome before 17.0.963.46 does not properly perform path clipping, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3963	Google Chrome before 17.0.963.46 does not properly handle PDF FAX images, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3964	Google Chrome before 17.0.963.46 does not properly implement the drag-and-drop feature, which makes it easier for remote attackers to spoof the URL bar via unspecified vectors.
CVE-2011-3965	Google Chrome before 17.0.963.46 does not properly check signatures, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2011-3966	Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to error handling for Cascading Style Sheets (CSS) token-sequence data.
CVE-2011-3967	Unspecified vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (application crash) via a crafted certificate.
CVE-2011-3968	Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving Cascading Style Sheets (CSS) token sequences.
CVE-2011-3969	Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to layout of SVG documents.

CVE-2011-3970	libxslt, as used in Google Chrome before 17.0.963.46, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3971	Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to mousemove events.
CVE-2011-3972	The shader translator implementation in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-4368	Cross-site scripting (XSS) vulnerability in Remote Development Services (RDS) in Adobe ColdFusion 8.0 through 9.0.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2011-4369	Unspecified vulnerability in the PRC component in Adobe Reader and Acrobat 9.x before 9.4.7 on Windows, Adobe Reader and Acrobat 9.x through 9.4.6 on Mac OS X, Adobe Reader and Acrobat 10.x through 10.1.1 on Windows and Mac OS X, and Adobe Reader 9.x through 9.4.6 on UNIX allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, as exploited in the wild in December 2011.
CVE-2011-4374	Integer overflow in Adobe Reader 9.x before 9.4.6 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-4681	Opera before 11.60 does not properly consider the number of . (dot) characters that conventionally exist in domain names of different top-level domains, which allows remote attackers to bypass the Same Origin Policy by leveraging access to a different domain name in the same top-level domain, as demonstrated by the .no or .uk domain.
CVE-2011-4682	The JavaScript engine in Opera before 11.60 does not properly implement the in operator, which allows remote attackers to bypass the Same Origin Policy via vectors related to variables on different web sites.
CVE-2011-4683	Unspecified vulnerability in Opera before 11.60 has unknown impact and attack vectors, related to a "moderately severe issue."
CVE-2011-4684	Opera before 11.60 does not properly handle certificate revocation, which has unspecified impact and remote attack vectors related to "corner cases."
CVE-2011-4685	Dragonfly in Opera before 11.60 allows remote attackers to cause a denial of service (application crash) via unspecified content on a web page, as demonstrated by forbes.com.

CVE-2011-4686	Unspecified vulnerability in the Web Workers implementation in Opera before 11.60 allows remote attackers to cause a denial of service (application crash) via unknown vectors.
CVE-2011-4687	Opera before 11.60 allows remote attackers to cause a denial of service (CPU and memory consumption) via unspecified content on a web page, as demonstrated by a page under the cisco.com home page.
CVE-2011-4690	Opera 11.60 and earlier does not prevent capture of data about the times of Same Origin Policy violations during IFRAME loading attempts, which makes it easier for remote attackers to determine whether a document exists in the browser cache via crafted JavaScript code.
CVE-2011-4691	Google Chrome 15.0.874.121 and earlier does not prevent capture of data about the times of Same Origin Policy violations during IFRAME loading attempts, which makes it easier for remote attackers to determine whether a document exists in the browser cache via crafted JavaScript code.
CVE-2011-4692	WebKit, as used in Apple Safari 5.1.1 and earlier and Google Chrome 15 and earlier, does not prevent capture of data about the time required for image loading, which makes it easier for remote attackers to determine whether an image exists in the browser cache via crafted JavaScript code, as demonstrated by visipisi.
CVE-2011-4708	Cross-site scripting (XSS) vulnerability in IBM Rational Asset Manager before 7.5.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2011-4800	Directory traversal vulnerability in Serv-U FTP Server before 11.1.0.5 allows remote authenticated users to read and write arbitrary files, and list and create arbitrary directories, via a "..:/" (dot dot colon forward slash) in the (1) list, (2) put, or (3) get commands.
CVE-2011-4890	The server in IBM solidDB 6.5 before FP9 and 7.0 before FP1 allows remote authenticated users to cause a denial of service (daemon crash) via a SELECT statement with a ROWNUM condition involving a subquery.
CVE-2011-5319	content/renderer/device_sensors/device_motion_event_pump.cc in Google Chrome before 41.0.2272.76 does not properly restrict access to high-rate accelerometer data, which makes it easier for remote attackers to capture keystrokes via a crafted web site that listens for ondevicemotion events, a different vulnerability than CVE-2015-1231.
CVE-2012-0135	Unspecified vulnerability in HP System Management Homepage (SMH) before 7.0 allows remote

	authenticated users to cause a denial of service via unknown vectors.
CVE-2012-0200	The server in IBM solidDB 6.5 before Interim Fix 6 does not properly initialize data structures, which allows remote authenticated users to cause a denial of service (daemon crash) via a SELECT statement with a redundant WHERE condition.
CVE-2012-0307	Multiple cross-site scripting (XSS) vulnerabilities in Symantec Messaging Gateway (SMG) before 10.0 allow remote attackers to inject arbitrary web script or HTML via (1) web content or (2) e-mail content.
CVE-2012-0308	Cross-site request forgery (CSRF) vulnerability in Symantec Messaging Gateway (SMG) before 10.0 allows remote attackers to hijack the authentication of administrators.
CVE-2012-0409	Multiple buffer overflows in EMC AutoStart 5.3.x and 5.4.x before 5.4.3 allow remote attackers to cause a denial of service (agent crash) or possibly execute arbitrary code via crafted packets.
CVE-2012-0428	Cross-site scripting (XSS) vulnerability in NetIQ eDirectory 8.8.6.x before 8.8.6.7 and 8.8.7.x before 8.8.7.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2012-0432	Stack-based buffer overflow in the Novell NCP implementation in NetIQ eDirectory 8.8.7.x before 8.8.7.2 allows remote attackers to have an unspecified impact via unknown vectors.
CVE-2012-0691	CA License (aka CA Licensing) before 1.90.03 does not properly restrict system commands, which allows local users to gain privileges via unspecified vectors.
CVE-2012-0692	CA License (aka CA Licensing) before 1.90.03 allows local users to modify or create arbitrary files, and consequently gain privileges, via unspecified vectors.
CVE-2012-0709	IBM DB2 9.5 before FP9, 9.7 through FP5, and 9.8 through FP4 does not properly check variables, which allows remote authenticated users to bypass intended restrictions on viewing table data by leveraging the CREATEIN privilege to execute crafted SQL CREATE VARIABLE statements.
CVE-2012-0710	IBM DB2 9.1 before FP11, 9.5 before FP9, 9.7 before FP5, and 9.8 before FP4 allows remote attackers to cause a denial of service (daemon crash) via a crafted Distributed Relational Database Architecture (DRDA) request.
CVE-2012-0711	Integer signedness error in the db2dasrrm process in the DB2 Administration Server (DAS) in IBM DB2 9.1 through FP11, 9.5 before FP9, and 9.7 through FP5 on UNIX platforms allows remote attackers to execute

	arbitrary code via a crafted request that triggers a heap-based buffer overflow.
CVE-2012-0712	The XML feature in IBM DB2 9.5 before FP9, 9.7 through FP5, and 9.8 through FP4 allows remote authenticated users to cause a denial of service (infinite loop) by calling the XMLPARSE function with a crafted string expression.
CVE-2012-0713	Unspecified vulnerability in the XML feature in IBM DB2 9.7 before FP6 on Linux, UNIX, and Windows allows remote authenticated users to read arbitrary XML files via unknown vectors.
CVE-2012-0724	Adobe Flash Player before 11.2.202.229 in Google Chrome before 18.0.1025.151 allow attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2012-0725.
CVE-2012-0725	Adobe Flash Player before 11.2.202.229 in Google Chrome before 18.0.1025.151 allow attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2012-0724.
CVE-2012-0726	The default configuration of TLS in IBM Tivoli Directory Server (TDS) 6.3 and earlier supports the (1) NULL-MD5 and (2) NULL-SHA ciphers, which allows remote attackers to trigger unencrypted communication via the TLS Handshake Protocol.
CVE-2012-0740	Cross-site scripting (XSS) vulnerability in the Web Admin Tool in IBM Tivoli Directory Server (TDS) 6.2 before 6.2.0.22 and 6.3 before 6.3.0.11 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2012-0743	IBM Tivoli Directory Server (TDS) 6.3 and earlier allows remote attackers to cause a denial of service (daemon crash) via a malformed LDAP paged search request.
CVE-2012-0752	Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to execute arbitrary code or cause a denial of service (memory corruption) by leveraging an unspecified "type confusion."
CVE-2012-0753	Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted MP4 data.
CVE-2012-0754	Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux,

	and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2012-0755	Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2012-0756.
CVE-2012-0756	Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2012-0755.
CVE-2012-0767	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Universal XSS (UXSS)," as exploited in the wild in February 2012.
CVE-2012-0768	The Matrix3D component in Adobe Flash Player before 10.3.183.16 and 11.x before 11.1.102.63 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.7 on Android 2.x and 3.x; and before 11.1.115.7 on Android 4.x allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2012-0769	Adobe Flash Player before 10.3.183.16 and 11.x before 11.1.102.63 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.7 on Android 2.x and 3.x; and before 11.1.115.7 on Android 4.x does not properly handle integers, which allows attackers to obtain sensitive information via unspecified vectors.
CVE-2012-0770	Adobe ColdFusion 8.0, 8.0.1, 9.0, and 9.0.1 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters.
CVE-2012-0773	The NetStream class in Adobe Flash Player before 10.3.183.18 and 11.x before 11.2.202.228 on Windows, Mac OS X, and Linux; Flash Player before 10.3.183.18 and 11.x before 11.2.202.223 on Solaris; Flash Player before 11.1.111.8 on Android 2.x and 3.x; and AIR before 3.2.0.2070 allows attackers to execute arbitrary

	code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2012-0774	Integer overflow in Adobe Reader and Acrobat 9.x before 9.5.1 and 10.x before 10.1.3 allows attackers to execute arbitrary code via a crafted TrueType font.
CVE-2012-0775	The JavaScript implementation in Adobe Reader and Acrobat 9.x before 9.5.1 and 10.x before 10.1.3 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2012-0776	The installer in Adobe Reader 9.x before 9.5.1 and 10.x before 10.1.3 allows attackers to bypass intended access restrictions and execute arbitrary code via unspecified vectors.
CVE-2012-0777	The JavaScript API in Adobe Reader and Acrobat 9.x before 9.5.1 and 10.x before 10.1.3 on Mac OS X and Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2012-0779	Adobe Flash Player before 10.3.183.19 and 11.x before 11.2.202.235 on Windows, Mac OS X, and Linux; before 11.1.111.9 on Android 2.x and 3.x; and before 11.1.115.8 on Android 4.x allows remote attackers to execute arbitrary code via a crafted file, related to an "object confusion vulnerability," as exploited in the wild in May 2012.
CVE-2012-1003	Multiple integer overflows in Opera 11.60 and earlier allow remote attackers to cause a denial of service (application crash) via a large integer argument to the (1) Int32Array, (2) Float32Array, (3) Float64Array, (4) Uint32Array, (5) Int16Array, or (6) ArrayBuffer function. NOTE: the vendor reportedly characterizes this as "a stability issue, not a security issue."
CVE-2012-1251	Opera before 9.63 does not properly verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2012-1521	Use-after-free vulnerability in the XML parser in Google Chrome before 18.0.1025.168 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-1530	Heap-based buffer overflow in the XSLT engine in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via a PDF file containing an XSL file that triggers memory corruption when the lang function processes XML data with a crafted node-set.
CVE-2012-1535	Unspecified vulnerability in Adobe Flash Player before 11.3.300.271 on Windows and Mac OS X and before

	11.2.202.238 on Linux allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted SWF content, as exploited in the wild in August 2012 with SWF content in a Word document.
CVE-2012-1796	Unspecified vulnerability in IBM Tivoli Monitoring Agent (ITMA), as used in IBM DB2 9.5 before FP9 on UNIX, allows local users to gain privileges via unknown vectors.
CVE-2012-1797	IBM DB2 9.5 uses world-writable permissions for nodes.reg, which has unspecified impact and attack vectors.
CVE-2012-1845	Use-after-free vulnerability in Google Chrome 17.0.963.66 and earlier allows remote attackers to bypass the DEP and ASLR protection mechanisms, and execute arbitrary code, via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2012. NOTE: the primary affected product may be clarified later; it was not identified by the researcher, who reportedly stated "it really doesn't matter if it's third-party code."
CVE-2012-1846	Google Chrome 17.0.963.66 and earlier allows remote attackers to bypass the sandbox protection mechanism by leveraging access to a sandboxed process, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2012. NOTE: the primary affected product may be clarified later; it was not identified by the researcher, who reportedly stated "it really doesn't matter if it's third-party code."
CVE-2012-1908	Cross-site scripting (XSS) vulnerability in Splunk 4.0 through 4.3 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.
CVE-2012-1924	Opera before 11.62 allows user-assisted remote attackers to trick users into downloading and executing arbitrary files via a small window for the download dialog.
CVE-2012-1925	Opera before 11.62 does not ensure that a dialog window is placed on top of content windows, which makes it easier for user-assisted remote attackers to trick users into downloading and executing arbitrary files via a download dialog located under other windows.
CVE-2012-1926	Opera before 11.62 allows remote attackers to bypass the Same Origin Policy via the (1) history.pushState and (2) history.replaceState functions in conjunction with cross-domain frames, leading to unintended read access to history.state information.
CVE-2012-1927	Opera before 11.62 allows remote attackers to spoof the address field by triggering the launch of a dialog window associated with a different domain.

CVE-2012-1928	Opera before 11.62 allows remote attackers to spoof the address field by triggering a page reload followed by a redirect to a different domain.
CVE-2012-1930	Opera before 11.62 on UNIX uses world-readable permissions for temporary files during printing, which allows local users to obtain sensitive information by reading these files.
CVE-2012-1931	Opera before 11.62 on UNIX, when used in conjunction with an unspecified printing application, allows local users to overwrite arbitrary files via a symlink attack on a temporary file during printing.
CVE-2012-1993	Unspecified vulnerability in HP System Management Homepage (SMH) before 7.0 allows local users to modify data or obtain sensitive information via unknown vectors.
CVE-2012-2000	Multiple unspecified vulnerabilities in HP System Health Application and Command Line Utilities before 9.0.0 allow remote attackers to execute arbitrary code via unknown vectors.
CVE-2012-2001	Cross-site scripting (XSS) vulnerability in HP SNMP Agents for Linux before 9.0.0 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2012-2002	Open redirect vulnerability in HP SNMP Agents for Linux before 9.0.0 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.
CVE-2012-2012	HP System Management Homepage (SMH) before 7.1.1 does not have an off autocomplete attribute for unspecified form fields, which makes it easier for remote attackers to obtain access by leveraging an unattended workstation.
CVE-2012-2013	Unspecified vulnerability in HP System Management Homepage (SMH) before 7.1.1 allows remote attackers to cause a denial of service, or possibly obtain sensitive information or modify data, via unknown vectors.
CVE-2012-2014	HP System Management Homepage (SMH) before 7.1.1 does not properly validate input, which allows remote authenticated users to have an unspecified impact via unknown vectors.
CVE-2012-2015	Unspecified vulnerability in HP System Management Homepage (SMH) before 7.1.1 allows remote authenticated users to gain privileges and obtain sensitive information via unknown vectors.
CVE-2012-2016	Unspecified vulnerability in HP System Management Homepage (SMH) before 7.1.1 allows local users to obtain sensitive information via unknown vectors.
CVE-2012-2034	Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X;

	before 10.3.183.20 and 11.x before 11.2.202.236 on Linux; before 11.1.111.10 on Android 2.x and 3.x; and before 11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-2037.
CVE-2012-2035	Stack-based buffer overflow in Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X; before 10.3.183.20 and 11.x before 11.2.202.236 on Linux; before 11.1.111.10 on Android 2.x and 3.x; and before 11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows attackers to execute arbitrary code via unspecified vectors.
CVE-2012-2036	Integer overflow in Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X; before 10.3.183.20 and 11.x before 11.2.202.236 on Linux; before 11.1.111.10 on Android 2.x and 3.x; and before 11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows attackers to execute arbitrary code via unspecified vectors.
CVE-2012-2037	Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X; before 10.3.183.20 and 11.x before 11.2.202.236 on Linux; before 11.1.111.10 on Android 2.x and 3.x; and before 11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-2034.
CVE-2012-2038	Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X; before 10.3.183.20 and 11.x before 11.2.202.236 on Linux; before 11.1.111.10 on Android 2.x and 3.x; and before 11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors.
CVE-2012-2039	Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X; before 10.3.183.20 and 11.x before 11.2.202.236 on Linux; before 11.1.111.10 on Android 2.x and 3.x; and before 11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows attackers to execute arbitrary code or cause a denial of service (NULL pointer dereference) via unspecified vectors.
CVE-2012-2040	Untrusted search path vulnerability in the installer in Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X; before 10.3.183.20 and 11.x before 11.2.202.236 on Linux; before 11.1.111.10 on Android 2.x and 3.x; and before

	11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows local users to gain privileges via a Trojan horse executable file in an unspecified directory.
CVE-2012-2041	CRLF injection vulnerability in the Component Browser in Adobe ColdFusion 8.0 through 9.0.1 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via unspecified vectors.
CVE-2012-2048	Unspecified vulnerability in Adobe ColdFusion 10 and earlier allows attackers to cause a denial of service via unknown vectors.
CVE-2012-2174	The URL handler in IBM Lotus Notes 8.x before 8.5.3 FP2 allows remote attackers to execute arbitrary code via a crafted notes:// URL.
CVE-2012-2180	The chaining functionality in the Distributed Relational Database Architecture (DRDA) module in IBM DB2 9.7 before FP6 and 9.8 before FP5 allows remote attackers to cause a denial of service (NULL pointer dereference, and resource consumption or daemon crash) via a crafted request.
CVE-2012-2194	Directory traversal vulnerability in the SQLJ.DB2_INSTALL_JAR stored procedure in IBM DB2 9.1 before FP12, 9.5 through FP9, 9.7 through FP6, 9.8 through FP5, and 10.1 allows remote attackers to replace JAR files via unspecified vectors.
CVE-2012-2196	IBM DB2 9.1 before FP12, 9.5 through FP9, 9.7 through FP6, 9.8 through FP5, and 10.1 allows remote attackers to read arbitrary XML files via the (1) GET_WRAP_CFG_C or (2) GET_WRAP_CFG_C2 stored procedure.
CVE-2012-2197	Stack-based buffer overflow in the Java Stored Procedure infrastructure in IBM DB2 9.1 before FP12, 9.5 through FP9, 9.7 through FP6, 9.8 through FP5, and 10.1 allows remote authenticated users to execute arbitrary code by leveraging certain CONNECT and EXECUTE privileges.
CVE-2012-2807	Multiple integer overflows in libxml2, as used in Google Chrome before 20.0.1132.43 and other products, on 64-bit Linux platforms allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-2815	Google Chrome before 20.0.1132.43 allows remote attackers to obtain potentially sensitive information from a fragment identifier by leveraging access to an IFRAME element associated with a different domain.
CVE-2012-2817	Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to tables that have sections.

CVE-2012-2818	Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the layout of documents that use the Cascading Style Sheets (CSS) counters feature.
CVE-2012-2819	The texSubImage2D implementation in the WebGL subsystem in Google Chrome before 20.0.1132.43 does not properly handle uploads to floating-point textures, which allows remote attackers to cause a denial of service (assertion failure and application crash) or possibly have unspecified other impact via a crafted web page, as demonstrated by certain WebGL performance tests, aka rdar problem 11520387.
CVE-2012-2820	Google Chrome before 20.0.1132.43 does not properly implement SVG filters, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-2821	The autofill implementation in Google Chrome before 20.0.1132.43 does not properly display text, which has unspecified impact and remote attack vectors.
CVE-2012-2822	The PDF functionality in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-2823	Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG resources.
CVE-2012-2824	Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG painting.
CVE-2012-2825	The XSL implementation in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service (incorrect read operation) via unspecified vectors.
CVE-2012-2826	Google Chrome before 20.0.1132.43 does not properly implement texture conversion, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-2828	Multiple integer overflows in the PDF functionality in Google Chrome before 20.0.1132.43 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2829	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the :first-letter pseudo-element.

CVE-2012-2830	Google Chrome before 20.0.1132.43 does not properly set array values, which allows remote attackers to cause a denial of service (incorrect pointer use) or possibly have unspecified other impact via unknown vectors.
CVE-2012-2831	Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG references.
CVE-2012-2832	The image-codec implementation in the PDF functionality in Google Chrome before 20.0.1132.43 does not initialize an unspecified pointer, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2012-2833	Buffer overflow in the JS API in the PDF functionality in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-2834	Integer overflow in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted data in the Matroska container format.
CVE-2012-2842	Use-after-free vulnerability in Google Chrome before 20.0.1132.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to counter handling.
CVE-2012-2843	Use-after-free vulnerability in Google Chrome before 20.0.1132.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to layout height tracking.
CVE-2012-2844	The PDF functionality in Google Chrome before 20.0.1132.57 does not properly handle JavaScript code, which allows remote attackers to cause a denial of service (incorrect object access) or possibly have unspecified other impact via a crafted document.
CVE-2012-2846	Google Chrome before 21.0.1180.57 on Linux does not properly isolate renderer processes, which allows remote attackers to cause a denial of service (cross-process interference) via unspecified vectors.
CVE-2012-2847	Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, does not request user confirmation before continuing a large series of downloads, which allows user-assisted remote attackers to cause a denial of service (resource consumption) via a crafted web site.
CVE-2012-2848	The drag-and-drop implementation in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and

	before 21.0.1180.60 on Windows and Chrome Frame, allows user-assisted remote attackers to bypass intended file access restrictions via a crafted web site.
CVE-2012-2849	Off-by-one error in the GIF decoder in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted image.
CVE-2012-2850	Multiple unspecified vulnerabilities in the PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allow remote attackers to have an unknown impact via a crafted document.
CVE-2012-2851	Multiple integer overflows in the PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2852	The PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, does not properly handle object linkage, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted document.
CVE-2012-2853	The webRequest API in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, does not properly interact with the Chrome Web Store, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site.
CVE-2012-2854	Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to obtain potentially sensitive information about pointer values by leveraging access to a WebUI renderer process.
CVE-2012-2855	Use-after-free vulnerability in the PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2856	The PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.

CVE-2012-2857	Use-after-free vulnerability in the Cascading Style Sheets (CSS) DOM implementation in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2858	Buffer overflow in the WebP decoder in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted WebP image.
CVE-2012-2859	Google Chrome before 21.0.1180.57 on Linux does not properly handle tabs, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors.
CVE-2012-2860	The date-picker implementation in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site.
CVE-2012-2862	Use-after-free vulnerability in the PDF functionality in Google Chrome before 21.0.1180.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2863	The PDF functionality in Google Chrome before 21.0.1180.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.
CVE-2012-2865	Google Chrome before 21.0.1180.89 does not properly perform line breaking, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.
CVE-2012-2866	Google Chrome before 21.0.1180.89 does not properly perform a cast of an unspecified variable during handling of run-in elements, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2012-2867	The SPDY implementation in Google Chrome before 21.0.1180.89 allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2012-2868	Race condition in Google Chrome before 21.0.1180.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving improper interaction between worker processes and an XMLHttpRequest (aka XHR) object.

CVE-2012-2869	Google Chrome before 21.0.1180.89 does not properly load URLs, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a "stale buffer."
CVE-2012-2870	libxslt 1.1.26 and earlier, as used in Google Chrome before 21.0.1180.89, does not properly manage memory, which might allow remote attackers to cause a denial of service (application crash) via a crafted XSLT expression that is not properly identified during XPath navigation, related to (1) the xsltCompileLocationPathPattern function in libxslt/pattern.c and (2) the xsltGenerateIdFunction function in libxslt/functions.c.
CVE-2012-2871	libxml2 2.9.0-rc1 and earlier, as used in Google Chrome before 21.0.1180.89, does not properly support a cast of an unspecified variable during handling of XSL transforms, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document, related to the _xmlNs data structure in include/libxml/tree.h.
CVE-2012-2872	Cross-site scripting (XSS) vulnerability in an SSL interstitial page in Google Chrome before 21.0.1180.89 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2012-2874	Skia, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an out-of-bounds write operation, a different vulnerability than CVE-2012-2883.
CVE-2012-2875	Multiple unspecified vulnerabilities in the PDF functionality in Google Chrome before 22.0.1229.79 allow remote attackers to have an unknown impact via a crafted document.
CVE-2012-2876	Buffer overflow in the SSE2 optimization functionality in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-2877	The extension system in Google Chrome before 22.0.1229.79 does not properly handle modal dialogs, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2012-2878	Use-after-free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to plug-in handling.
CVE-2012-2879	Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service (DOM topology corruption) via a crafted document.

CVE-2012-2880	Race condition in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the plug-in paint buffer.
CVE-2012-2881	Google Chrome before 22.0.1229.79 does not properly handle plug-ins, which allows remote attackers to cause a denial of service (DOM tree corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2012-2882	FFmpeg, as used in Google Chrome before 22.0.1229.79, does not properly handle OGG containers, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, related to a "wild pointer" issue.
CVE-2012-2883	Skia, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an out-of-bounds write operation, a different vulnerability than CVE-2012-2874.
CVE-2012-2884	Skia, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-2885	Double free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to application exit.
CVE-2012-2886	Cross-site scripting (XSS) vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to inject arbitrary web script or HTML via vectors related to the Google V8 bindings, aka "Universal XSS (UXSS)."
CVE-2012-2887	Use-after-free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving onclick events.
CVE-2012-2888	Use-after-free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG text references.
CVE-2012-2889	Cross-site scripting (XSS) vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to inject arbitrary web script or HTML via vectors involving frames, aka "Universal XSS (UXSS)."
CVE-2012-2890	Use-after-free vulnerability in the PDF functionality in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2891	The IPC implementation in Google Chrome before 22.0.1229.79 allows attackers to obtain potentially

	sensitive information about memory addresses via unspecified vectors.
CVE-2012-2892	Unspecified vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2012-2893	Double free vulnerability in libxslt, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XSL transforms.
CVE-2012-2894	Google Chrome before 22.0.1229.79 does not properly handle graphics-context data structures, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2012-2895	The PDF functionality in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.
CVE-2012-2900	Skia, as used in Google Chrome before 22.0.1229.92, does not properly render text, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2012-2942	Buffer overflow in the trash buffer in the header capture functionality in HAProxy before 1.4.21, when global.tune.bufsize is set to a value greater than the default and header rewriting is enabled, allows remote attackers to cause a denial of service and possibly execute arbitrary code via unspecified vectors.
CVE-2012-3319	IBM Rational Business Developer 8.x before 8.0.1.4 allows remote attackers to obtain potentially sensitive information via a connection to a web service created with the Rational Business Developer product.
CVE-2012-3579	Symantec Messaging Gateway (SMG) before 10.0 has a default password for an unspecified account, which makes it easier for remote attackers to obtain privileged access via an SSH session.
CVE-2012-3580	Symantec Messaging Gateway (SMG) before 10.0 allows remote authenticated users to modify the web application by leveraging access to the management interface.
CVE-2012-3581	Symantec Messaging Gateway (SMG) before 10.0 allows remote attackers to obtain potentially sensitive information about component versions via unspecified vectors.
CVE-2012-3845	Buffer overflow in LAN Messenger 1.2.28 and earlier allows remote attackers to cause a denial of service (crash) via a long string in an initiation request.

CVE-2012-4010	Opera before 11.60 allows remote attackers to spoof the address bar via unspecified homograph characters, a different vulnerability than CVE-2010-2660.
CVE-2012-4142	Opera before 12.01 on Windows and UNIX, and before 11.66 and 12.x before 12.01 on Mac OS X, ignores some characters in HTML documents in unspecified circumstances, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via a crafted document.
CVE-2012-4143	Opera before 12.01 on Windows and UNIX, and before 11.66 and 12.x before 12.01 on Mac OS X, allows user-assisted remote attackers to trick users into downloading and executing arbitrary files via a small window for the download dialog, a different vulnerability than CVE-2012-1924.
CVE-2012-4144	Opera before 12.01 on Windows and UNIX, and before 11.66 and 12.x before 12.01 on Mac OS X, does not properly escape characters in DOM elements, which makes it easier for remote attackers to bypass cross-site scripting (XSS) protection mechanisms via a crafted HTML document.
CVE-2012-4145	Unspecified vulnerability in Opera before 12.01 on Windows and UNIX, and before 11.66 and 12.x before 12.01 on Mac OS X, has unknown impact and attack vectors, related to a "low severity issue."
CVE-2012-4146	Opera before 12.01 allows remote attackers to cause a denial of service (application crash) via a crafted web site, as demonstrated by the Lenovo "Shop now" page.
CVE-2012-4163	Adobe Flash Player before 10.3.183.23 and 11.x before 11.4.402.265 on Windows and Mac OS X, before 10.3.183.23 and 11.x before 11.2.202.238 on Linux, before 11.1.111.16 on Android 2.x and 3.x, and before 11.1.115.17 on Android 4.x; Adobe AIR before 3.4.0.2540; and Adobe AIR SDK before 3.4.0.2540 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-4164 and CVE-2012-4165.
CVE-2012-4164	Adobe Flash Player before 10.3.183.23 and 11.x before 11.4.402.265 on Windows and Mac OS X, before 10.3.183.23 and 11.x before 11.2.202.238 on Linux, before 11.1.111.16 on Android 2.x and 3.x, and before 11.1.115.17 on Android 4.x; Adobe AIR before 3.4.0.2540; and Adobe AIR SDK before 3.4.0.2540 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-4163 and CVE-2012-4165.
CVE-2012-4165	Adobe Flash Player before 10.3.183.23 and 11.x before 11.4.402.265 on Windows and Mac OS X,

	before 10.3.183.23 and 11.x before 11.2.202.238 on Linux, before 11.1.111.16 on Android 2.x and 3.x, and before 11.1.115.17 on Android 4.x; Adobe AIR before 3.4.0.2540; and Adobe AIR SDK before 3.4.0.2540 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-4163 and CVE-2012-4164.
CVE-2012-4167	Integer overflow in Adobe Flash Player before 10.3.183.23 and 11.x before 11.4.402.265 on Windows and Mac OS X, before 10.3.183.23 and 11.x before 11.2.202.238 on Linux, before 11.1.111.16 on Android 2.x and 3.x, and before 11.1.115.17 on Android 4.x; Adobe AIR before 3.4.0.2540; and Adobe AIR SDK before 3.4.0.2540 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2012-4168	Adobe Flash Player before 10.3.183.23 and 11.x before 11.4.402.265 on Windows and Mac OS X, before 10.3.183.23 and 11.x before 11.2.202.238 on Linux, before 11.1.111.16 on Android 2.x and 3.x, and before 11.1.115.17 on Android 4.x; Adobe AIR before 3.4.0.2540; and Adobe AIR SDK before 3.4.0.2540 allow remote attackers to read content from a different domain via a crafted web site.
CVE-2012-4171	Adobe Flash Player before 10.3.183.23 and 11.x before 11.4.402.265 on Windows and Mac OS X, before 10.3.183.23 and 11.x before 11.2.202.238 on Linux, before 11.1.111.16 on Android 2.x and 3.x, and before 11.1.115.17 on Android 4.x; Adobe AIR before 3.4.0.2540; and Adobe AIR SDK before 3.4.0.2540 allow attackers to cause a denial of service (application crash) by leveraging a logic error during handling of Firefox dialogs.
CVE-2012-4347	Multiple directory traversal vulnerabilities in the management console in Symantec Messaging Gateway (SMG) 9.5.x allow remote authenticated users to read arbitrary files via a .. (dot dot) in the (1) logFile parameter in a logs action to brightmail/export or (2) localBackupFileSelection parameter in an APPLIANCE restoreSource action to brightmail/admin/restore/download.do.
CVE-2012-4607	Buffer overflow in nsrindexd in EMC NetWorker 7.5.x and 7.6.x before 7.6.5, and 8.x before 8.0.0.6, allows remote attackers to execute arbitrary code via crafted SunRPC data.
CVE-2012-4826	Stack-based buffer overflow in the SQL/PSM (aka SQL Persistent Stored Module) Stored Procedure (SP) infrastructure in IBM DB2 9.1, 9.5, 9.7 before FP7, 9.8, and 10.1 might allow remote authenticated users to execute arbitrary code by debugging a stored procedure.

CVE-2012-4842	Open redirect vulnerability in the web server in IBM Lotus Domino 8.5.x through 8.5.3 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.
CVE-2012-4844	Cross-site scripting (XSS) vulnerability in the web server in IBM Lotus Domino 8.5.x through 8.5.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2012-4846	IBM Lotus Notes 8.5.x before 8.5.3 FP3 does not include the HTTPOnly flag in a Set-Cookie header for a web-application cookie, which makes it easier for remote attackers to obtain potentially sensitive information via script access to this cookie, aka SPRs JMAS7TRNLN and SRAO8U3Q68.
CVE-2012-4862	The Host Connect emulator in IBM Rational Developer for System z 7.1 through 8.5.1 does not properly store the SSL certificate password, which allows local users to obtain sensitive information via unspecified vectors.
CVE-2012-4956	Heap-based buffer overflow in NFRAgent.exe in Novell File Reporter 1.0.2 allows remote attackers to execute arbitrary code via a large number of VOL elements in an SRS record.
CVE-2012-4957	Absolute path traversal vulnerability in NFRAgent.exe in Novell File Reporter 1.0.2 allows remote attackers to read arbitrary files via a /FSF/CMD request with a full pathname in a PATH element of an SRS record.
CVE-2012-4958	Directory traversal vulnerability in NFRAgent.exe in Novell File Reporter 1.0.2 allows remote attackers to read arbitrary files via a 126 /FSF/CMD request with a .. (dot dot) in a FILE element of an FSFUI record.
CVE-2012-4959	Directory traversal vulnerability in NFRAgent.exe in Novell File Reporter 1.0.2 allows remote attackers to upload and execute files via a 130 /FSF/CMD request with a .. (dot dot) in a FILE element of an FSFUI record.
CVE-2012-5054	Integer overflow in the copyRawDataTo method in the Matrix3D class in Adobe Flash Player before 11.4.402.265 allows remote attackers to execute arbitrary code via malformed arguments.
CVE-2012-5108	Race condition in Google Chrome before 22.0.1229.92 allows remote attackers to execute arbitrary code via vectors related to audio devices.
CVE-2012-5109	The International Components for Unicode (ICU) functionality in Google Chrome before 22.0.1229.92 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to a regular expression.
CVE-2012-5110	The compositor in Google Chrome before 22.0.1229.92 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.

CVE-2012-5111	Google Chrome before 22.0.1229.92 does not monitor for crashes of Pepper plug-ins, which has unspecified impact and remote attack vectors.
CVE-2012-5112	Use-after-free vulnerability in the SVG implementation in WebKit, as used in Google Chrome before 22.0.1229.94, allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2012-5116	Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of SVG filters.
CVE-2012-5117	Google Chrome before 23.0.1271.64 does not properly restrict the loading of an SVG subresource in the context of an IMG element, which has unspecified impact and remote attack vectors.
CVE-2012-5119	Race condition in Pepper, as used in Google Chrome before 23.0.1271.64, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to buffers.
CVE-2012-5120	Google V8 before 3.13.7.5, as used in Google Chrome before 23.0.1271.64, on 64-bit Linux platforms allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers an out-of-bounds access to an array.
CVE-2012-5121	Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to video layout.
CVE-2012-5122	Google Chrome before 23.0.1271.64 does not properly perform a cast of an unspecified variable during handling of input, which allows remote attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2012-5123	Skia, as used in Google Chrome before 23.0.1271.64, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-5124	Google Chrome before 23.0.1271.64 does not properly handle textures, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2012-5125	Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of extension tabs.
CVE-2012-5126	Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of plug-in placeholders.

CVE-2012-5127	Integer overflow in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted WebP image.
CVE-2012-5128	Google V8 before 3.13.7.5, as used in Google Chrome before 23.0.1271.64, does not properly perform write operations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-5130	Skia, as used in Google Chrome before 23.0.1271.91, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-5132	Google Chrome before 23.0.1271.91 allows remote attackers to cause a denial of service (application crash) via a response with chunked transfer coding.
CVE-2012-5133	Use-after-free vulnerability in Google Chrome before 23.0.1271.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG filters.
CVE-2012-5134	Heap-based buffer underflow in the xmlParseAttValueComplex function in parser.c in libxml2 2.9.0 and earlier, as used in Google Chrome before 23.0.1271.91 and other products, allows remote attackers to cause a denial of service or possibly execute arbitrary code via crafted entities in an XML document.
CVE-2012-5135	Use-after-free vulnerability in Google Chrome before 23.0.1271.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to printing.
CVE-2012-5136	Google Chrome before 23.0.1271.91 does not properly perform a cast of an unspecified variable during handling of the INPUT element, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted HTML document.
CVE-2012-5137	Use-after-free vulnerability in Google Chrome before 23.0.1271.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the Media Source API.
CVE-2012-5138	Google Chrome before 23.0.1271.95 does not properly handle file paths, which has unspecified impact and attack vectors.
CVE-2012-5139	Use-after-free vulnerability in Google Chrome before 23.0.1271.97 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to visibility events.
CVE-2012-5140	Use-after-free vulnerability in Google Chrome before 23.0.1271.97 allows remote attackers to cause a denial

	of service or possibly have unspecified other impact via vectors related to the URL loader.
CVE-2012-5141	Google Chrome before 23.0.1271.97 does not properly restrict instantiation of the Chromoting client plug-in, which has unspecified impact and attack vectors.
CVE-2012-5142	Google Chrome before 23.0.1271.97 does not properly handle history navigation, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors.
CVE-2012-5143	Integer overflow in Google Chrome before 23.0.1271.97 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to PPAPI image buffers.
CVE-2012-5144	Google Chrome before 23.0.1271.97, and Libav 0.7.x before 0.7.7 and 0.8.x before 0.8.5, do not properly perform AAC decoding, which allows remote attackers to cause a denial of service (stack memory corruption) or possibly have unspecified other impact via vectors related to "an off-by-one overwrite when switching to LTP profile from MAIN."
CVE-2012-5145	Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG layout.
CVE-2012-5146	Google Chrome before 24.0.1312.52 allows remote attackers to bypass the Same Origin Policy via a malformed URL.
CVE-2012-5147	Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOM handling.
CVE-2012-5148	The hyphenation functionality in Google Chrome before 24.0.1312.52 does not properly validate file names, which has unspecified impact and attack vectors.
CVE-2012-5149	Integer overflow in the audio IPC layer in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-5150	Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving seek operations on video data.
CVE-2012-5151	Integer overflow in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code in a PDF document.
CVE-2012-5152	Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (out-of-bounds

	read) via vectors involving seek operations on video data.
CVE-2012-5153	Google V8 before 3.14.5.3, as used in Google Chrome before 24.0.1312.52, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers an out-of-bounds access to stack memory.
CVE-2012-5156	Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving PDF fields.
CVE-2012-5157	Google Chrome before 24.0.1312.52 does not properly handle image data in PDF documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.
CVE-2012-5248	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5249	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5250	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5251	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK

	before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5252	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5253	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5254	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5255	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5256	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a

	denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5257	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5258	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5259	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5260	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5261	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified

	vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5262	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5263	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5264	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5265	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5266	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability

	than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5267	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5268	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5269	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5270	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5271	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified

	vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5272	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5274	Buffer overflow in Adobe Flash Player before 10.3.183.43 and 11.x before 11.5.502.110 on Windows and Mac OS X, before 10.3.183.43 and 11.x before 11.2.202.251 on Linux, before 11.1.111.24 on Android 2.x and 3.x, and before 11.1.115.27 on Android 4.x; Adobe AIR before 3.5.0.600; and Adobe AIR SDK before 3.5.0.600 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2012-5275, CVE-2012-5276, CVE-2012-5277, and CVE-2012-5280.
CVE-2012-5275	Buffer overflow in Adobe Flash Player before 10.3.183.43 and 11.x before 11.5.502.110 on Windows and Mac OS X, before 10.3.183.43 and 11.x before 11.2.202.251 on Linux, before 11.1.111.24 on Android 2.x and 3.x, and before 11.1.115.27 on Android 4.x; Adobe AIR before 3.5.0.600; and Adobe AIR SDK before 3.5.0.600 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2012-5274, CVE-2012-5276, CVE-2012-5277, and CVE-2012-5280.
CVE-2012-5276	Buffer overflow in Adobe Flash Player before 10.3.183.43 and 11.x before 11.5.502.110 on Windows and Mac OS X, before 10.3.183.43 and 11.x before 11.2.202.251 on Linux, before 11.1.111.24 on Android 2.x and 3.x, and before 11.1.115.27 on Android 4.x; Adobe AIR before 3.5.0.600; and Adobe AIR SDK before 3.5.0.600 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2012-5274, CVE-2012-5275, CVE-2012-5277, and CVE-2012-5280.
CVE-2012-5277	Buffer overflow in Adobe Flash Player before 10.3.183.43 and 11.x before 11.5.502.110 on Windows and Mac OS X, before 10.3.183.43 and 11.x before 11.2.202.251 on Linux, before 11.1.111.24 on Android 2.x and 3.x, and before 11.1.115.27 on Android 4.x; Adobe AIR before 3.5.0.600; and Adobe AIR SDK before 3.5.0.600 allows attackers to execute arbitrary code via unspecified vectors, a different

	vulnerability than CVE-2012-5274, CVE-2012-5275, CVE-2012-5276, and CVE-2012-5280.
CVE-2012-5278	Adobe Flash Player before 10.3.183.43 and 11.x before 11.5.502.110 on Windows and Mac OS X, before 10.3.183.43 and 11.x before 11.2.202.251 on Linux, before 11.1.111.24 on Android 2.x and 3.x, and before 11.1.115.27 on Android 4.x; Adobe AIR before 3.5.0.600; and Adobe AIR SDK before 3.5.0.600 allow attackers to bypass intended access restrictions and execute arbitrary code via unspecified vectors.
CVE-2012-5279	Adobe Flash Player before 10.3.183.43 and 11.x before 11.5.502.110 on Windows and Mac OS X, before 10.3.183.43 and 11.x before 11.2.202.251 on Linux, before 11.1.111.24 on Android 2.x and 3.x, and before 11.1.115.27 on Android 4.x; Adobe AIR before 3.5.0.600; and Adobe AIR SDK before 3.5.0.600 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2012-5280	Buffer overflow in Adobe Flash Player before 10.3.183.43 and 11.x before 11.5.502.110 on Windows and Mac OS X, before 10.3.183.43 and 11.x before 11.2.202.251 on Linux, before 11.1.111.24 on Android 2.x and 3.x, and before 11.1.115.27 on Android 4.x; Adobe AIR before 3.5.0.600; and Adobe AIR SDK before 3.5.0.600 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2012-5274, CVE-2012-5275, CVE-2012-5276, and CVE-2012-5277.
CVE-2012-5285	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5286	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5287	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before

	11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5376	The Inter-process Communication (IPC) implementation in Google Chrome before 22.0.1229.94 allows remote attackers to bypass intended sandbox restrictions and write to arbitrary files by leveraging access to a renderer process, a different vulnerability than CVE-2012-5112.
CVE-2012-5673	Unspecified vulnerability in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 has unknown impact and attack vectors.
CVE-2012-5675	Adobe ColdFusion 9.0 through 9.0.2, and 10, allows local users to bypass intended shared-hosting sandbox permissions via unspecified vectors.
CVE-2012-5676	Buffer overflow in Adobe Flash Player before 10.3.183.48 and 11.x before 11.5.502.135 on Windows, before 10.3.183.48 and 11.x before 11.5.502.136 on Mac OS X, before 10.3.183.48 and 11.x before 11.2.202.258 on Linux, before 11.1.111.29 on Android 2.x and 3.x, and before 11.1.115.34 on Android 4.x; Adobe AIR before 3.5.0.880 on Windows and before 3.5.0.890 on Mac OS X; and Adobe AIR SDK before 3.5.0.880 on Windows and before 3.5.0.890 on Mac OS X allows attackers to execute arbitrary code via unspecified vectors.
CVE-2012-5677	Integer overflow in Adobe Flash Player before 10.3.183.48 and 11.x before 11.5.502.135 on Windows, before 10.3.183.48 and 11.x before 11.5.502.136 on Mac OS X, before 10.3.183.48 and 11.x before 11.2.202.258 on Linux, before 11.1.111.29 on Android 2.x and 3.x, and before 11.1.115.34 on Android 4.x; Adobe AIR before 3.5.0.880 on Windows and before 3.5.0.890 on Mac OS X; and Adobe AIR SDK before 3.5.0.880 on Windows and before 3.5.0.890 on Mac OS X allows attackers to execute arbitrary code via unspecified vectors.
CVE-2012-5678	Adobe Flash Player before 10.3.183.48 and 11.x before 11.5.502.135 on Windows, before 10.3.183.48 and 11.x before 11.5.502.136 on Mac OS X, before 10.3.183.48 and 11.x before 11.2.202.258 on Linux, before 11.1.111.29 on Android 2.x and 3.x, and

	before 11.1.115.34 on Android 4.x; Adobe AIR before 3.5.0.880 on Windows and before 3.5.0.890 on Mac OS X; and Adobe AIR SDK before 3.5.0.880 on Windows and before 3.5.0.890 on Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2012-5851	html/parser/XSSAuditor.cpp in WebCore in WebKit, as used in Google Chrome through 22 and Safari 5.1.7, does not consider all possible output contexts of reflected data, which makes it easier for remote attackers to bypass a cross-site scripting (XSS) protection mechanism via a crafted string, aka rdar problem 12019108.
CVE-2012-5956	Multiple cross-site scripting (XSS) vulnerabilities in ManageEngine AssetExplorer 5.6 before service pack 5614 allow remote attackers to inject arbitrary web script or HTML via fields in XML asset data to discoveryServlet/WsDiscoveryServlet, as demonstrated by the DocRoot/Computer_Information/output element.
CVE-2012-6460	Opera before 11.67 and 12.x before 12.02 allows remote attackers to cause truncation of a dialog, and possibly trigger downloading and execution of arbitrary programs, via a crafted web site.
CVE-2012-6461	The X.509 certificate-validation functionality in the https implementation in Opera before 12.10 allows remote attackers to trigger a false indication of successful revocation-status checking by causing a failure of a single checking service.
CVE-2012-6462	Opera before 12.10 does not properly implement the Cross-Origin Resource Sharing (CORS) specification, which allows remote attackers to bypass intended page-content restrictions via a crafted request.
CVE-2012-6463	Cross-site scripting (XSS) vulnerability in Opera before 12.10 allows remote attackers to inject arbitrary web script or HTML via vectors involving an unspecified sequence of loading of documents and loading of data: URLs.
CVE-2012-6464	Cross-site scripting (XSS) vulnerability in Opera before 12.10 allows remote attackers to inject arbitrary web script or HTML via crafted JavaScript code that overrides methods of unspecified native objects in documents that have different origins.
CVE-2012-6465	Opera before 12.10 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a malformed SVG image.
CVE-2012-6466	Opera before 12.10 does not properly handle incorrect size data in a WebP image, which allows remote attackers to obtain potentially sensitive information from process memory by using a crafted image as the fill pattern for a canvas.

CVE-2012-6467	Opera before 12.10 follows Internet shortcuts that are referenced by a (1) IMG element or (2) other inline element, which makes it easier for remote attackers to conduct phishing attacks via a crafted web site, as exploited in the wild in November 2012.
CVE-2012-6468	Heap-based buffer overflow in Opera before 12.11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a long HTTP response.
CVE-2012-6469	Opera before 12.11 allows remote attackers to determine the existence of arbitrary local files via vectors involving web script in an error page.
CVE-2012-6470	Opera before 12.12 does not properly allocate memory for GIF images, which allows remote attackers to execute arbitrary code or cause a denial of service (memory overwrite) via a malformed image.
CVE-2012-6471	Opera before 12.12 allows remote attackers to spoof the address field via a high rate of HTTP requests.
CVE-2012-6472	Opera before 12.12 on UNIX uses weak permissions for the profile directory, which allows local users to obtain sensitive information by reading a (1) cache file, (2) password file, or (3) configuration file, or (4) possibly gain privileges by modifying or overwriting a configuration file.
CVE-2013-0471	The traditional scheduler in the client in IBM Tivoli Storage Manager (TSM) before 6.2.5.0, 6.3 before 6.3.1.0, and 6.4 before 6.4.0.1, when Prompted mode is enabled, allows remote attackers to cause a denial of service (scheduling outage) via unspecified vectors.
CVE-2013-0472	The Web GUI in the client in IBM Tivoli Storage Manager (TSM) 6.3 before 6.3.1.0 and 6.4 before 6.4.0.1 allows man-in-the-middle attackers to obtain unspecified client access, and consequently obtain unspecified server access, via unknown vectors.
CVE-2013-0504	Buffer overflow in the broker service in Adobe Flash Player before 10.3.183.67 and 11.x before 11.6.602.171 on Windows and Mac OS X, and before 10.3.183.67 and 11.x before 11.2.202.273 on Linux, allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-0601	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-1530, CVE-2013-0605, CVE-2013-0616, CVE-2013-0619, CVE-2013-0620, and CVE-2013-0623.
CVE-2013-0602	Use-after-free vulnerability in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x

	before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-0603	Heap-based buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0604.
CVE-2013-0604	Heap-based buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0603.
CVE-2013-0605	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-1530, CVE-2013-0601, CVE-2013-0616, CVE-2013-0619, CVE-2013-0620, and CVE-2013-0623.
CVE-2013-0606	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0612, CVE-2013-0615, CVE-2013-0617, and CVE-2013-0621.
CVE-2013-0607	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to execute arbitrary code via unspecified vectors, related to a "logic error," a different vulnerability than CVE-2013-0608, CVE-2013-0611, CVE-2013-0614, and CVE-2013-0618.
CVE-2013-0608	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to execute arbitrary code via unspecified vectors, related to a "logic error," a different vulnerability than CVE-2013-0607, CVE-2013-0611, CVE-2013-0614, and CVE-2013-0618.
CVE-2013-0609	Integer overflow in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0613.
CVE-2013-0610	Stack-based buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0626.
CVE-2013-0611	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to execute arbitrary code via unspecified vectors,

	related to a "logic error," a different vulnerability than CVE-2013-0607, CVE-2013-0608, CVE-2013-0614, and CVE-2013-0618.
CVE-2013-0612	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0606, CVE-2013-0615, CVE-2013-0617, and CVE-2013-0621.
CVE-2013-0613	Integer overflow in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0609.
CVE-2013-0614	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to execute arbitrary code via unspecified vectors, related to a "logic error," a different vulnerability than CVE-2013-0607, CVE-2013-0608, CVE-2013-0611, and CVE-2013-0618.
CVE-2013-0615	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0606, CVE-2013-0612, CVE-2013-0617, and CVE-2013-0621.
CVE-2013-0616	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-1530, CVE-2013-0601, CVE-2013-0605, CVE-2013-0619, CVE-2013-0620, and CVE-2013-0623.
CVE-2013-0617	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0606, CVE-2013-0612, CVE-2013-0615, and CVE-2013-0621.
CVE-2013-0618	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to execute arbitrary code via unspecified vectors, related to a "logic error," a different vulnerability than CVE-2013-0607, CVE-2013-0608, CVE-2013-0611, and CVE-2013-0614.
CVE-2013-0619	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-1530, CVE-2013-0601,

	CVE-2013-0605, CVE-2013-0616, CVE-2013-0620, and CVE-2013-0623.
CVE-2013-0620	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-1530, CVE-2013-0601, CVE-2013-0605, CVE-2013-0616, CVE-2013-0619, and CVE-2013-0623.
CVE-2013-0621	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0606, CVE-2013-0612, CVE-2013-0615, and CVE-2013-0617.
CVE-2013-0622	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2013-0624.
CVE-2013-0623	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-1530, CVE-2013-0601, CVE-2013-0605, CVE-2013-0616, CVE-2013-0619, and CVE-2013-0620.
CVE-2013-0624	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2013-0622.
CVE-2013-0625	Adobe ColdFusion 9.0, 9.0.1, and 9.0.2, when a password is not configured, allows remote attackers to bypass authentication and possibly execute arbitrary code via unspecified vectors, as exploited in the wild in January 2013.
CVE-2013-0626	Stack-based buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0610.
CVE-2013-0627	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows local users to gain privileges via unknown vectors.
CVE-2013-0629	Adobe ColdFusion 9.0, 9.0.1, 9.0.2, and 10, when a password is not configured, allows attackers to access restricted directories via unspecified vectors, as exploited in the wild in January 2013.

CVE-2013-0630	Buffer overflow in Adobe Flash Player before 10.3.183.50 and 11.x before 11.5.502.146 on Windows and Mac OS X, before 10.3.183.50 and 11.x before 11.2.202.261 on Linux, before 11.1.111.31 on Android 2.x and 3.x, and before 11.1.115.36 on Android 4.x; Adobe AIR before 3.5.0.1060; and Adobe AIR SDK before 3.5.0.1060 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-0631	Adobe ColdFusion 9.0, 9.0.1, and 9.0.2 allows attackers to obtain sensitive information via unspecified vectors, as exploited in the wild in January 2013.
CVE-2013-0632	administrator.cfc in Adobe ColdFusion 9.0, 9.0.1, 9.0.2, and 10 allows remote attackers to bypass authentication and possibly execute arbitrary code by logging in to the RDS component using the default empty password and leveraging this session to access the administrative web interface, as exploited in the wild in January 2013.
CVE-2013-0633	Buffer overflow in Adobe Flash Player before 10.3.183.51 and 11.x before 11.5.502.149 on Windows and Mac OS X, before 10.3.183.51 and 11.x before 11.2.202.262 on Linux, before 11.1.111.32 on Android 2.x and 3.x, and before 11.1.115.37 on Android 4.x allows remote attackers to execute arbitrary code via crafted SWF content, as exploited in the wild in February 2013.
CVE-2013-0634	Adobe Flash Player before 10.3.183.51 and 11.x before 11.5.502.149 on Windows and Mac OS X, before 10.3.183.51 and 11.x before 11.2.202.262 on Linux, before 11.1.111.32 on Android 2.x and 3.x, and before 11.1.115.37 on Android 4.x allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted SWF content, as exploited in the wild in February 2013.
CVE-2013-0637	Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allow attackers to obtain sensitive information via unspecified vectors.
CVE-2013-0638	Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allow attackers to execute arbitrary code or cause a denial of

	service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-0647.
CVE-2013-0639	Integer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-0640	Adobe Reader and Acrobat 9.x before 9.5.4, 10.x before 10.1.6, and 11.x before 11.0.02 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted PDF document, as exploited in the wild in February 2013.
CVE-2013-0641	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.4, 10.x before 10.1.6, and 11.x before 11.0.02 allows remote attackers to execute arbitrary code via a crafted PDF document, as exploited in the wild in February 2013.
CVE-2013-0642	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0645, CVE-2013-1365, CVE-2013-1366, CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, CVE-2013-1372, and CVE-2013-1373.
CVE-2013-0643	The Firefox sandbox in Adobe Flash Player before 10.3.183.67 and 11.x before 11.6.602.171 on Windows and Mac OS X, and before 10.3.183.67 and 11.x before 11.2.202.273 on Linux, does not properly restrict privileges, which makes it easier for remote attackers to execute arbitrary code via crafted SWF content, as exploited in the wild in February 2013.
CVE-2013-0644	Use-after-free vulnerability in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0649 and CVE-2013-1374.

CVE-2013-0645	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0642, CVE-2013-1365, CVE-2013-1366, CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, CVE-2013-1372, and CVE-2013-1373.
CVE-2013-0646	Integer overflow in Adobe Flash Player before 10.3.183.68 and 11.x before 11.6.602.180 on Windows and Mac OS X, before 10.3.183.68 and 11.x before 11.2.202.275 on Linux, before 11.1.111.44 on Android 2.x and 3.x, and before 11.1.115.48 on Android 4.x; Adobe AIR before 3.6.0.6090; Adobe AIR SDK before 3.6.0.6090; and Adobe AIR SDK & Compiler before 3.6.0.6090 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-0647	Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-0638.
CVE-2013-0648	Unspecified vulnerability in the ExternalInterface ActionScript functionality in Adobe Flash Player before 10.3.183.67 and 11.x before 11.6.602.171 on Windows and Mac OS X, and before 10.3.183.67 and 11.x before 11.2.202.273 on Linux, allows remote attackers to execute arbitrary code via crafted SWF content, as exploited in the wild in February 2013.
CVE-2013-0649	Use-after-free vulnerability in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0644 and CVE-2013-1374.
CVE-2013-0650	Use-after-free vulnerability in Adobe Flash Player before 10.3.183.68 and 11.x before 11.6.602.180 on

	Windows and Mac OS X, before 10.3.183.68 and 11.x before 11.2.202.275 on Linux, before 11.1.111.44 on Android 2.x and 3.x, and before 11.1.115.48 on Android 4.x; Adobe AIR before 3.6.0.6090; Adobe AIR SDK before 3.6.0.6090; and Adobe AIR SDK & Compiler before 3.6.0.6090 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-0828	The PDF functionality in Google Chrome before 24.0.1312.52 does not properly perform a cast of an unspecified variable during processing of the root of the structure tree, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2013-0829	Google Chrome before 24.0.1312.52 does not properly maintain database metadata, which allows remote attackers to bypass intended file-access restrictions via unspecified vectors.
CVE-2013-0831	Directory traversal vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to have an unspecified impact by leveraging access to an extension process.
CVE-2013-0832	Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to printing.
CVE-2013-0833	Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to printing.
CVE-2013-0834	Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors involving glyphs.
CVE-2013-0835	Unspecified vulnerability in the Geolocation implementation in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (application crash) via unknown vectors.
CVE-2013-0836	Google V8 before 3.14.5.3, as used in Google Chrome before 24.0.1312.52, does not properly implement garbage collection, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2013-0837	Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of extension tabs.
CVE-2013-0838	Google Chrome before 24.0.1312.52 on Linux uses weak permissions for shared memory segments, which has unspecified impact and attack vectors.

CVE-2013-0839	Use-after-free vulnerability in Google Chrome before 24.0.1312.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of fonts in CANVAS elements.
CVE-2013-0840	Google Chrome before 24.0.1312.56 does not validate URLs during the opening of new windows, which has unspecified impact and remote attack vectors.
CVE-2013-0841	Array index error in the content-blocking functionality in Google Chrome before 24.0.1312.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0842	Google Chrome before 24.0.1312.56 does not properly handle %00 characters in pathnames, which has unspecified impact and attack vectors.
CVE-2013-0879	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly implement web audio nodes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-0880	Use-after-free vulnerability in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to databases.
CVE-2013-0881	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (incorrect read operation) via crafted data in the Matroska container format.
CVE-2013-0882	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (incorrect memory access) or possibly have unspecified other impact via a large number of SVG parameters.
CVE-2013-0883	Skia, as used in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (incorrect read operation) via unspecified vectors.
CVE-2013-0884	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly load Native Client (aka NaCl) code, which has unspecified impact and attack vectors.
CVE-2013-0885	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly restrict API privileges during interaction with

	the Chrome Web Store, which has unspecified impact and attack vectors.
CVE-2013-0887	The developer-tools process in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly restrict privileges during interaction with a connected server, which has unspecified impact and attack vectors.
CVE-2013-0888	Skia, as used in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to a "user gesture check for dangerous file downloads."
CVE-2013-0889	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly enforce a user gesture requirement before proceeding with a file download, which might make it easier for remote attackers to execute arbitrary code via a crafted file.
CVE-2013-0890	Multiple unspecified vulnerabilities in the IPC layer in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allow remote attackers to cause a denial of service (memory corruption) or possibly have other impact via unknown vectors.
CVE-2013-0891	Integer overflow in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a blob.
CVE-2013-0892	Multiple unspecified vulnerabilities in the IPC layer in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allow remote attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-0893	Race condition in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to media.
CVE-2013-0894	Buffer overflow in the vorbis_parse_setup_hdr_floors function in the Vorbis decoder in vorbisdec.c in libavcodec in FFmpeg through 1.1.3, as used in Google Chrome before 25.0.1364.97 on Windows and Linux and before 25.0.1364.99 on Mac OS X and other products, allows remote attackers to cause a denial of service (divide-by-zero error or out-of-bounds array access) or possibly have unspecified other impact via vectors involving a zero value for a bark map size.
CVE-2013-0895	Google Chrome before 25.0.1364.97 on Linux, and before 25.0.1364.99 on Mac OS X, does not properly

	handle pathnames during copy operations, which might make it easier for remote attackers to execute arbitrary programs via unspecified vectors.
CVE-2013-0896	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly manage memory during message handling for plug-ins, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0897	Off-by-one error in the PDF functionality in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service via a crafted document.
CVE-2013-0898	Use-after-free vulnerability in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a URL.
CVE-2013-0899	Integer overflow in the padding implementation in the opus_packet_parse_impl function in src/opus_decoder.c in Opus before 1.0.2, as used in Google Chrome before 25.0.1364.97 on Windows and Linux and before 25.0.1364.99 on Mac OS X and other products, allows remote attackers to cause a denial of service (out-of-bounds read) via a long packet.
CVE-2013-0900	Race condition in the International Components for Unicode (ICU) functionality in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0902	Use-after-free vulnerability in the frame-loader implementation in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0903	Use-after-free vulnerability in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of browser navigation.
CVE-2013-0904	The Web Audio implementation in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-0905	Use-after-free vulnerability in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving an SVG animation.

CVE-2013-0906	The IndexedDB implementation in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-0907	Race condition in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of media threads.
CVE-2013-0908	Google Chrome before 25.0.1364.152 does not properly manage bindings of extension processes, which has unspecified impact and attack vectors.
CVE-2013-0909	The XSS Auditor in Google Chrome before 25.0.1364.152 allows remote attackers to obtain sensitive HTTP Referer information via unspecified vectors.
CVE-2013-0910	Google Chrome before 25.0.1364.152 does not properly manage the interaction between the browser process and renderer processes during authorization of the loading of a plug-in, which makes it easier for remote attackers to bypass intended access restrictions via vectors involving a blocked plug-in.
CVE-2013-0911	Directory traversal vulnerability in Google Chrome before 25.0.1364.152 allows remote attackers to have an unspecified impact via vectors related to databases.
CVE-2013-0912	WebKit in Google Chrome before 25.0.1364.160 allows remote attackers to execute arbitrary code via vectors that leverage "type confusion."
CVE-2013-0916	Use-after-free vulnerability in the Web Audio implementation in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0917	The URL loader in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2013-0918	Google Chrome before 26.0.1410.43 does not prevent navigation to developer tools in response to a drag-and-drop operation, which allows user-assisted remote attackers to have an unspecified impact via a crafted web site.
CVE-2013-0919	Use-after-free vulnerability in Google Chrome before 26.0.1410.43 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging the presence of an extension that creates a pop-up window.
CVE-2013-0920	Use-after-free vulnerability in the extension bookmarks API in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service or

	possibly have unspecified other impact via unknown vectors.
CVE-2013-0921	The Isolated Sites feature in Google Chrome before 26.0.1410.43 does not properly enforce the use of separate processes, which makes it easier for remote attackers to bypass intended access restrictions via a crafted web site.
CVE-2013-0922	Google Chrome before 26.0.1410.43 does not properly restrict brute-force access attempts against web sites that require HTTP Basic Authentication, which has unspecified impact and attack vectors.
CVE-2013-0923	The USB Apps API in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-0924	The extension functionality in Google Chrome before 26.0.1410.43 does not verify that use of the permissions API is consistent with file permissions, which has unspecified impact and attack vectors.
CVE-2013-0925	Google Chrome before 26.0.1410.43 does not ensure that an extension has the tabs (aka APIPermission::kTab) permission before providing a URL to this extension, which has unspecified impact and remote attack vectors.
CVE-2013-0926	Google Chrome before 26.0.1410.43 does not properly handle active content in an EMBED element during a copy-and-paste operation, which allows user-assisted remote attackers to have an unspecified impact via a crafted web site.
CVE-2013-0940	The nsrpush process in the client in EMC NetWorker before 7.6.5.3 and 8.x before 8.0.1.4 sets weak permissions for unspecified files, which allows local users to gain privileges via unknown vectors.
CVE-2013-1365	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0642, CVE-2013-0645, CVE-2013-1366, CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, CVE-2013-1372, and CVE-2013-1373.
CVE-2013-1366	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android

	2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0642, CVE-2013-0645, CVE-2013-1365, CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, CVE-2013-1372, and CVE-2013-1373.
CVE-2013-1367	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0642, CVE-2013-0645, CVE-2013-1365, CVE-2013-1366, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, CVE-2013-1372, and CVE-2013-1373.
CVE-2013-1368	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0642, CVE-2013-0645, CVE-2013-1365, CVE-2013-1366, CVE-2013-1367, CVE-2013-1369, CVE-2013-1370, CVE-2013-1372, and CVE-2013-1373.
CVE-2013-1369	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0642, CVE-2013-0645, CVE-2013-1365, CVE-2013-1366, CVE-2013-1367, CVE-2013-1368, CVE-2013-1370, CVE-2013-1372, and CVE-2013-1373.
CVE-2013-1370	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android

	2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0642, CVE-2013-0645, CVE-2013-1365, CVE-2013-1366, CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1372, and CVE-2013-1373.
CVE-2013-1371	Adobe Flash Player before 10.3.183.68 and 11.x before 11.6.602.180 on Windows and Mac OS X, before 10.3.183.68 and 11.x before 11.2.202.275 on Linux, before 11.1.111.44 on Android 2.x and 3.x, and before 11.1.115.48 on Android 4.x; Adobe AIR before 3.6.0.6090; Adobe AIR SDK before 3.6.0.6090; and Adobe AIR SDK & Compiler before 3.6.0.6090 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-1372	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0642, CVE-2013-0645, CVE-2013-1365, CVE-2013-1366, CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, and CVE-2013-1373.
CVE-2013-1373	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0642, CVE-2013-0645, CVE-2013-1365, CVE-2013-1366, CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, and CVE-2013-1372.
CVE-2013-1374	Use-after-free vulnerability in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute

	arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0644 and CVE-2013-0649.
CVE-2013-1375	Heap-based buffer overflow in Adobe Flash Player before 10.3.183.68 and 11.x before 11.6.602.180 on Windows and Mac OS X, before 10.3.183.68 and 11.x before 11.2.202.275 on Linux, before 11.1.111.44 on Android 2.x and 3.x, and before 11.1.115.48 on Android 4.x; Adobe AIR before 3.6.0.6090; Adobe AIR SDK before 3.6.0.6090; and Adobe AIR SDK & Compiler before 3.6.0.6090 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-1378	Adobe Flash Player before 10.3.183.75 and 11.x before 11.7.700.169 on Windows and Mac OS X, before 10.3.183.75 and 11.x before 11.2.202.280 on Linux, before 11.1.111.50 on Android 2.x and 3.x, and before 11.1.115.54 on Android 4.x; Adobe AIR before 3.7.0.1530; and Adobe AIR SDK & Compiler before 3.7.0.1530 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-1380.
CVE-2013-1379	Adobe Flash Player before 10.3.183.75 and 11.x before 11.7.700.169 on Windows and Mac OS X, before 10.3.183.75 and 11.x before 11.2.202.280 on Linux, before 11.1.111.50 on Android 2.x and 3.x, and before 11.1.115.54 on Android 4.x; Adobe AIR before 3.7.0.1530; and Adobe AIR SDK & Compiler before 3.7.0.1530 do not properly initialize pointer arrays, which allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-1380	Adobe Flash Player before 10.3.183.75 and 11.x before 11.7.700.169 on Windows and Mac OS X, before 10.3.183.75 and 11.x before 11.2.202.280 on Linux, before 11.1.111.50 on Android 2.x and 3.x, and before 11.1.115.54 on Android 4.x; Adobe AIR before 3.7.0.1530; and Adobe AIR SDK & Compiler before 3.7.0.1530 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-1378.
CVE-2013-1618	The TLS implementation in Opera before 12.13 does not properly consider timing side-channel attacks on a MAC check operation during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, a related issue to CVE-2013-0169.
CVE-2013-1637	Opera before 12.13 allows remote attackers to execute arbitrary code via vectors involving DOM events.

CVE-2013-1638	Opera before 12.13 allows remote attackers to execute arbitrary code via crafted clipPaths in an SVG document.
CVE-2013-1639	Opera before 12.13 does not send CORS preflight requests in all required cases, which allows remote attackers to bypass a CSRF protection mechanism via a crafted web site that triggers a CORS request.
CVE-2013-2268	Unspecified vulnerability in the MathML implementation in WebKit in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, has unknown impact and remote attack vectors, related to a "high severity security issue."
CVE-2013-2503	Privoxy before 3.0.21 does not properly handle Proxy-Authenticate and Proxy-Authorization headers in the client-server data stream, which makes it easier for remote HTTP servers to spoof the intended proxy service via a 407 (aka Proxy Authentication Required) HTTP status code.
CVE-2013-2549	Unspecified vulnerability in Adobe Reader 11.0.02 allows remote attackers to execute arbitrary code via vectors related to a "break into the sandbox," as demonstrated by George Hotz during a Pwn2Own competition at CanSecWest 2013.
CVE-2013-2550	Unspecified vulnerability in Adobe Reader 11.0.02 allows attackers to bypass the sandbox protection mechanism via unknown vectors, as demonstrated by George Hotz during a Pwn2Own competition at CanSecWest 2013.
CVE-2013-2555	Integer overflow in Adobe Flash Player before 10.3.183.75 and 11.x before 11.7.700.169 on Windows and Mac OS X, before 10.3.183.75 and 11.x before 11.2.202.280 on Linux, before 11.1.111.50 on Android 2.x and 3.x, and before 11.1.115.54 on Android 4.x; Adobe AIR before 3.7.0.1530; and Adobe AIR SDK & Compiler before 3.7.0.1530 allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2013.
CVE-2013-2632	Google V8 before 3.17.13, as used in Google Chrome before 27.0.1444.3, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code, as demonstrated by the Bejeweled game.
CVE-2013-2718	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726,

	CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2719	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2720	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2721	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2722	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2723	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of

	service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2724	Stack-based buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-2725	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2726	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2727	Integer overflow in Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-2729.
CVE-2013-2728	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331,

	CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.
CVE-2013-2729	Integer overflow in Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-2727.
CVE-2013-2730	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-2733.
CVE-2013-2731	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2732	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2733	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-2730.
CVE-2013-2734	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.

CVE-2013-2735	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2736	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2737	A JavaScript API in Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allows attackers to obtain sensitive information via unspecified vectors.
CVE-2013-2738	minidlna has SQL Injection that may allow retrieval of arbitrary files
CVE-2013-2739	MiniDLNA has heap-based buffer overflow
CVE-2013-2741	importbuddy.php in the BackupBuddy plugin 1.3.4, 2.1.4, 2.2.25, 2.2.28, and 2.2.4 for WordPress does not require that authentication be enabled, which allows remote attackers to obtain sensitive information, or overwrite or delete files, via vectors involving a (1) direct request, (2) step=1 request, (3) step=2 or step=3 request, or (4) step=7 request.
CVE-2013-2766	Cross-site scripting (XSS) vulnerability in Splunk Web in Splunk 4.3.0 through 4.3.5 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2013-2836	Multiple unspecified vulnerabilities in Google Chrome before 27.0.1453.93 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2837	Use-after-free vulnerability in the SVG implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

CVE-2013-2838	Google V8, as used in Google Chrome before 27.0.1453.93, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2013-2839	Google Chrome before 27.0.1453.93 does not properly perform a cast of an unspecified variable during handling of clipboard data, which allows remote attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2840	Use-after-free vulnerability in the media loader in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2013-2846.
CVE-2013-2841	Use-after-free vulnerability in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of Pepper resources.
CVE-2013-2842	Use-after-free vulnerability in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of widgets.
CVE-2013-2843	Use-after-free vulnerability in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of speech data.
CVE-2013-2844	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to style resolution.
CVE-2013-2845	The Web Audio implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2846	Use-after-free vulnerability in the media loader in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2013-2840.
CVE-2013-2847	Race condition in the workers implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2848	The XSS Auditor in Google Chrome before 27.0.1453.93 might allow remote attackers to obtain sensitive information via unspecified vectors.
CVE-2013-2849	Multiple cross-site scripting (XSS) vulnerabilities in Google Chrome before 27.0.1453.93 allow user-

	assisted remote attackers to inject arbitrary web script or HTML via vectors involving a (1) drag-and-drop or (2) copy-and-paste operation.
CVE-2013-2853	The HTTPS implementation in Google Chrome before 28.0.1500.71 does not ensure that headers are terminated by \r\n\r\n (carriage return, newline, carriage return, newline), which allows man-in-the-middle attackers to have an unspecified impact via vectors that trigger header truncation.
CVE-2013-2855	The Developer Tools API in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2856	Use-after-free vulnerability in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of input.
CVE-2013-2857	Use-after-free vulnerability in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of images.
CVE-2013-2858	Use-after-free vulnerability in the HTML5 Audio implementation in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2859	Google Chrome before 27.0.1453.110 allows remote attackers to bypass the Same Origin Policy and trigger namespace pollution via unspecified vectors.
CVE-2013-2860	Use-after-free vulnerability in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving access to a database API by a worker process.
CVE-2013-2861	Use-after-free vulnerability in the SVG implementation in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2862	Skia, as used in Google Chrome before 27.0.1453.110, does not properly handle GPU acceleration, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2863	Google Chrome before 27.0.1453.110 does not properly handle SSL sockets, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-2864	The PDF functionality in Google Chrome before 27.0.1453.110 allows remote attackers to cause a

	denial of service (invalid free operation) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2865	Multiple unspecified vulnerabilities in Google Chrome before 27.0.1453.110 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2867	Google Chrome before 28.0.1500.71 does not properly prevent pop-under windows, which allows remote attackers to have an unspecified impact via a crafted web site.
CVE-2013-2868	common/extensions/sync_helper.cc in Google Chrome before 28.0.1500.71 proceeds with sync operations for NPAPI extensions without checking for a certain plugin permission setting, which might allow remote attackers to trigger unwanted extension changes via unspecified vectors.
CVE-2013-2869	Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted JPEG2000 image.
CVE-2013-2870	Use-after-free vulnerability in Google Chrome before 28.0.1500.71 allows remote servers to execute arbitrary code via crafted response traffic after a URL request.
CVE-2013-2871	Use-after-free vulnerability in Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of input.
CVE-2013-2873	Use-after-free vulnerability in Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a 404 HTTP status code during the loading of resources.
CVE-2013-2875	core/rendering/svg/SVGInlineTextBox.cpp in the SVG implementation in Blink, as used in Google Chrome before 28.0.1500.71, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2013-2876	browser/extensions/api/tabs/tabs_api.cc in Google Chrome before 28.0.1500.71 does not properly enforce restrictions on the capture of screenshots by extensions, which allows remote attackers to obtain sensitive information about the content of a previous page via vectors involving an interstitial page.
CVE-2013-2877	parser.c in libxml2 before 2.9.0, as used in Google Chrome before 28.0.1500.71 and other products, allows remote attackers to cause a denial of service (out-of-bounds read) via a document that ends abruptly, related to the lack of certain checks for the XML_PARSER_EOF state.

CVE-2013-2878	Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the handling of text.
CVE-2013-2879	Google Chrome before 28.0.1500.71 does not properly determine the circumstances in which a renderer process can be considered a trusted process for sign-in and subsequent sync operations, which makes it easier for remote attackers to conduct phishing attacks via a crafted web site.
CVE-2013-2880	Multiple unspecified vulnerabilities in Google Chrome before 28.0.1500.71 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2881	Google Chrome before 28.0.1500.95 does not properly handle frames, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2013-2882	Google V8, as used in Google Chrome before 28.0.1500.95, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2013-2883	Use-after-free vulnerability in Google Chrome before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to deleting the registration of a MutationObserver object.
CVE-2013-2884	Use-after-free vulnerability in the DOM implementation in Google Chrome before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to improper tracking of which document owns an Attr object.
CVE-2013-2885	Use-after-free vulnerability in Google Chrome before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to not properly considering focus during the processing of JavaScript events in the presence of a multiple-fields input type.
CVE-2013-2886	Multiple unspecified vulnerabilities in Google Chrome before 28.0.1500.95 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2887	Multiple unspecified vulnerabilities in Google Chrome before 29.0.1547.57 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2900	The FilePath::ReferencesParent function in files/file_path.cc in Google Chrome before 29.0.1547.57 on Windows does not properly handle pathname components composed entirely of . (dot) and whitespace characters, which allows remote attackers

	to conduct directory traversal attacks via a crafted directory name.
CVE-2013-2901	Multiple integer overflows in (1) libGLESv2/renderer/Renderer9.cpp and (2) libGLESv2/renderer/Renderer11.cpp in Almost Native Graphics Layer Engine (ANGLE), as used in Google Chrome before 29.0.1547.57, allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2902	Use-after-free vulnerability in the XSLT ProcessingInstruction implementation in Blink, as used in Google Chrome before 29.0.1547.57, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to an applyXSLTransform call involving (1) an HTML document or (2) an xsl:processing-instruction element that is still in the process of loading.
CVE-2013-2903	Use-after-free vulnerability in the HTMLMediaElement::didMoveToNewDocument function in core/html/HTMLMediaElement.cpp in Blink, as used in Google Chrome before 29.0.1547.57, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving moving a (1) AUDIO or (2) VIDEO element between documents.
CVE-2013-2904	Use-after-free vulnerability in the Document::finishedParsing function in core/dom/Document.cpp in Blink, as used in Google Chrome before 29.0.1547.57, allows remote attackers to cause a denial of service or possibly have unspecified other impact via an onload event that changes an IFRAME element so that its src attribute is no longer an XML document, leading to unintended garbage collection of this document.
CVE-2013-2905	The SharedMemory::Create function in memory/shared_memory_posix.cc in Google Chrome before 29.0.1547.57 uses weak permissions under /dev/shm/, which allows attackers to obtain sensitive information via direct access to a POSIX shared-memory file.
CVE-2013-2906	Multiple race conditions in the Web Audio implementation in Blink, as used in Google Chrome before 30.0.1599.66, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to threading in core/html/HTMLMediaElement.cpp, core/platform/audio/AudioDSPKernelProcessor.cpp, core/platform/audio/HRTFElevation.cpp, and modules/webaudio/ConvolverNode.cpp.
CVE-2013-2907	The Window.prototype object implementation in Google Chrome before 30.0.1599.66 allows remote attackers

	to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2013-2908	Google Chrome before 30.0.1599.66 uses incorrect function calls to determine the values of NavigationEntry objects, which allows remote attackers to spoof the address bar via vectors involving a response with a 204 (aka No Content) status code.
CVE-2013-2909	Use-after-free vulnerability in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to inline-block rendering for bidirectional Unicode text in an element isolated from its siblings.
CVE-2013-2910	Use-after-free vulnerability in modules/webaudio/AudioScheduledSourceNode.cpp in the Web Audio implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2911	Use-after-free vulnerability in the XSLStyleSheet::compileStyleSheet function in core/xml/XSLStyleSheetLibxslt.cpp in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of post-failure recompilation in unspecified libxslt versions.
CVE-2013-2912	Use-after-free vulnerability in the PepperInProcessRouter::SendToHost function in content/renderer/pepper/pepper_in_process_router.cc in the Pepper Plug-in API (PPAPI) in Google Chrome before 30.0.1599.66 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a resource-destruction message.
CVE-2013-2913	Use-after-free vulnerability in the XMLDocumentParser::append function in core/xml/parser/XMLDocumentParser.cpp in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving an XML document.
CVE-2013-2915	Google Chrome before 30.0.1599.66 preserves pending NavigationEntry objects in certain invalid circumstances, which allows remote attackers to spoof the address bar via a URL with a malformed scheme, as demonstrated by a nonexistent:12121 URL.
CVE-2013-2916	Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to spoof the address bar via vectors involving a response with a 204 (aka No

	Content) status code, in conjunction with a delay in notifying the user of an attempted spoof.
CVE-2013-2917	The ReverbConvolverStage::ReverbConvolverStage function in core/platform/audio/ReverbConvolverStage.cpp in the Web Audio implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the impulseResponse array.
CVE-2013-2918	Use-after-free vulnerability in the RenderBlock::collapseAnonymousBlockChild function in core/rendering/RenderBlock.cpp in the DOM implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect handling of parent-child relationships for anonymous blocks.
CVE-2013-2919	Google V8, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2920	The DoResolveRelativeHost function in url/url_canon_relative.cc in Google Chrome before 30.0.1599.66 allows remote attackers to cause a denial of service (out-of-bounds read) via a relative URL containing a hostname, as demonstrated by a protocol-relative URL beginning with a //www.google.com/ substring.
CVE-2013-2921	Double free vulnerability in the ResourceFetcher::didLoadResource function in core/fetch/ResourceFetcher.cpp in the resource loader in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering certain callback processing during the reporting of a resource entry.
CVE-2013-2922	Use-after-free vulnerability in core/html/HTMLTemplateElement.cpp in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that operates on a TEMPLATE element.
CVE-2013-2923	Multiple unspecified vulnerabilities in Google Chrome before 30.0.1599.66 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2924	Use-after-free vulnerability in International Components for Unicode (ICU), as used in Google Chrome before 30.0.1599.66 and other products, allows remote

	attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2925	Use-after-free vulnerability in core/xml/XMLHttpRequest.cpp in Blink, as used in Google Chrome before 30.0.1599.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger multiple conflicting uses of the same XMLHttpRequest object.
CVE-2013-2926	Use-after-free vulnerability in the IndentOutdentCommand::tryIndentingAsListItem function in core/editing/IndentOutdentCommand.cpp in Blink, as used in Google Chrome before 30.0.1599.101, allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to list elements.
CVE-2013-2927	Use-after-free vulnerability in the HTMLFormElement::prepareForSubmission function in core/html/HTMLFormElement.cpp in Blink, as used in Google Chrome before 30.0.1599.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to submission for FORM elements.
CVE-2013-2928	Multiple unspecified vulnerabilities in Google Chrome before 30.0.1599.101 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2931	Multiple unspecified vulnerabilities in Google Chrome before 31.0.1650.48 allow attackers to execute arbitrary code or possibly have other impact via unknown vectors.
CVE-2013-3210	Opera before 12.15 does not properly block top-level domains in Set-Cookie headers, which allows remote attackers to obtain sensitive information by leveraging control of a different web site in the same top-level domain.
CVE-2013-3211	Unspecified vulnerability in Opera before 12.15 has unknown impact and attack vectors, related to a "moderately severe issue."
CVE-2013-3324	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331,

	CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.
CVE-2013-3325	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.
CVE-2013-3326	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.
CVE-2013-3327	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.
CVE-2013-3328	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory

	corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.
CVE-2013-3329	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.
CVE-2013-3330	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.
CVE-2013-3331	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.
CVE-2013-3332	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and

	3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.
CVE-2013-3333	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3334, and CVE-2013-3335.
CVE-2013-3334	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, and CVE-2013-3335.
CVE-2013-3337	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-3338	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of

	service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-3339	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-3340	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, and CVE-2013-3341.
CVE-2013-3341	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, and CVE-2013-3340.
CVE-2013-3342	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 do not properly handle operating-system domain blacklists, which has unspecified impact and attack vectors.
CVE-2013-3343	Adobe Flash Player before 10.3.183.90 and 11.x before 11.7.700.224 on Windows, before 10.3.183.90 and 11.x before 11.7.700.225 on Mac OS X, before 10.3.183.90 and 11.x before 11.2.202.291 on Linux, before 11.1.111.59 on Android 2.x and 3.x, and before 11.1.115.63 on Android 4.x; Adobe AIR before

	3.7.0.2090 on Windows and Android and before 3.7.0.2100 on Mac OS X; and Adobe AIR SDK & Compiler before 3.7.0.2090 on Windows and before 3.7.0.2100 on Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-3344	Heap-based buffer overflow in Adobe Flash Player before 11.7.700.232 and 11.8.x before 11.8.800.94 on Windows and Mac OS X, before 11.2.202.297 on Linux, before 11.1.111.64 on Android 2.x and 3.x, and before 11.1.115.69 on Android 4.x allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-3345	Adobe Flash Player before 11.7.700.232 and 11.8.x before 11.8.800.94 on Windows and Mac OS X, before 11.2.202.297 on Linux, before 11.1.111.64 on Android 2.x and 3.x, and before 11.1.115.69 on Android 4.x allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-3346	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-3347	Integer overflow in Adobe Flash Player before 11.7.700.232 and 11.8.x before 11.8.800.94 on Windows and Mac OS X, before 11.2.202.297 on Linux, before 11.1.111.64 on Android 2.x and 3.x, and before 11.1.115.69 on Android 4.x allows attackers to execute arbitrary code via PCM data that is not properly handled during resampling.
CVE-2013-3361	Adobe Flash Player before 11.7.700.242 and 11.8.x before 11.8.800.168 on Windows and Mac OS X, before 11.2.202.310 on Linux, before 11.1.111.73 on Android 2.x and 3.x, and before 11.1.115.81 on Android 4.x; Adobe AIR before 3.8.0.1430; and Adobe AIR SDK & Compiler before 3.8.0.1430 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-3362, CVE-2013-3363, and CVE-2013-5324.
CVE-2013-3362	Adobe Flash Player before 11.7.700.242 and 11.8.x before 11.8.800.168 on Windows and Mac OS X, before 11.2.202.310 on Linux, before 11.1.111.73 on Android 2.x and 3.x, and before 11.1.115.81 on Android

	4.x; Adobe AIR before 3.8.0.1430; and Adobe AIR SDK & Compiler before 3.8.0.1430 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-3361, CVE-2013-3363, and CVE-2013-5324.
CVE-2013-3363	Adobe Flash Player before 11.7.700.242 and 11.8.x before 11.8.800.168 on Windows and Mac OS X, before 11.2.202.310 on Linux, before 11.1.111.73 on Android 2.x and 3.x, and before 11.1.115.81 on Android 4.x; Adobe AIR before 3.8.0.1430; and Adobe AIR SDK & Compiler before 3.8.0.1430 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-3361, CVE-2013-3362, and CVE-2013-5324.
CVE-2013-5324	Adobe Flash Player before 11.7.700.242 and 11.8.x before 11.8.800.168 on Windows and Mac OS X, before 11.2.202.310 on Linux, before 11.1.111.73 on Android 2.x and 3.x, and before 11.1.115.81 on Android 4.x; Adobe AIR before 3.8.0.1430; and Adobe AIR SDK & Compiler before 3.8.0.1430 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-3361, CVE-2013-3362, and CVE-2013-3363.
CVE-2013-5329	Adobe Flash Player before 11.7.700.252 and 11.8.x and 11.9.x before 11.9.900.152 on Windows and Mac OS X and before 11.2.202.327 on Linux, Adobe AIR before 3.9.0.1210, Adobe AIR SDK before 3.9.0.1210, and Adobe AIR SDK & Compiler before 3.9.0.1210 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-5330.
CVE-2013-5330	Adobe Flash Player before 11.7.700.252 and 11.8.x and 11.9.x before 11.9.900.152 on Windows and Mac OS X and before 11.2.202.327 on Linux, Adobe AIR before 3.9.0.1210, Adobe AIR SDK before 3.9.0.1210, and Adobe AIR SDK & Compiler before 3.9.0.1210 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-5329.
CVE-2013-5331	Adobe Flash Player before 11.7.700.257 and 11.8.x and 11.9.x before 11.9.900.170 on Windows and Mac OS X and before 11.2.202.332 on Linux, Adobe AIR before 3.9.0.1380, Adobe AIR SDK before 3.9.0.1380, and Adobe AIR SDK & Compiler before 3.9.0.1380 allow remote attackers to execute arbitrary code via crafted .swf content that leverages an unspecified "type confusion," as exploited in the wild in December 2013.

CVE-2013-5332	Adobe Flash Player before 11.7.700.257 and 11.8.x and 11.9.x before 11.9.900.170 on Windows and Mac OS X and before 11.2.202.332 on Linux, Adobe AIR before 3.9.0.1380, Adobe AIR SDK before 3.9.0.1380, and Adobe AIR SDK & Compiler before 3.9.0.1380 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-6166	Google Chrome before 29 sends HTTP Cookie headers without first validating that they have the required character-set restrictions, which allows remote attackers to conduct the equivalent of a persistent Logout CSRF attack via a crafted parameter that forces a web application to set a malformed cookie within an HTTP response.
CVE-2013-6621	Use-after-free vulnerability in Google Chrome before 31.0.1650.48 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the x-webkit-speech attribute in a text INPUT element.
CVE-2013-6622	Use-after-free vulnerability in the HTMLMediaElement::didMoveToNewDocument function in core/html/HTMLMediaElement.cpp in Blink, as used in Google Chrome before 31.0.1650.48, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the movement of a media element between documents.
CVE-2013-6623	The SVG implementation in Blink, as used in Google Chrome before 31.0.1650.48, allows remote attackers to cause a denial of service (out-of-bounds read) by leveraging the use of tree order, rather than transitive dependency order, for layout.
CVE-2013-6624	Use-after-free vulnerability in Google Chrome before 31.0.1650.48 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the string values of id attributes.
CVE-2013-6625	Use-after-free vulnerability in core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 31.0.1650.48, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of DOM range objects in circumstances that require child node removal after a (1) mutation or (2) blur event.
CVE-2013-6626	The WebContentsImpl::AttachInterstitialPage function in content/browser/web_contents/web_contents_impl.cc in Google Chrome before 31.0.1650.48 does not cancel JavaScript dialogs upon generating an interstitial warning, which allows remote attackers to spoof the address bar via a crafted web site.

CVE-2013-6627	net/http/http_stream_parser.cc in Google Chrome before 31.0.1650.48 does not properly process HTTP Informational (aka 1xx) status codes, which allows remote web servers to cause a denial of service (out-of-bounds read) via a crafted response.
CVE-2013-6628	net/socket/ssl_client_socket_nss.cc in the TLS implementation in Google Chrome before 31.0.1650.48 does not ensure that a server's X.509 certificate is the same during renegotiation as it was before renegotiation, which might allow remote web servers to interfere with trust relationships by renegotiating a session.
CVE-2013-6629	The get_sos function in jdmarker.c in (1) libjpeg 6b and (2) libjpeg-turbo through 1.3.0, as used in Google Chrome before 31.0.1650.48, Ghostscript, and other products, does not check for certain duplications of component data during the reading of segments that follow Start Of Scan (SOS) JPEG markers, which allows remote attackers to obtain sensitive information from uninitialized memory locations via a crafted JPEG image.
CVE-2013-6630	The get_dht function in jdmarker.c in libjpeg-turbo through 1.3.0, as used in Google Chrome before 31.0.1650.48 and other products, does not set all elements of a certain Huffman value array during the reading of segments that follow Define Huffman Table (DHT) JPEG markers, which allows remote attackers to obtain sensitive information from uninitialized memory locations via a crafted JPEG image.
CVE-2013-6631	Use-after-free vulnerability in the Channel::SendRTCPPacket function in voice_engine/channel.cc in libjingle in WebRTC, as used in Google Chrome before 31.0.1650.48 and other products, allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via vectors that trigger the absence of certain statistics initialization, leading to the skipping of a required DeRegisterExternalTransport call.
CVE-2013-6632	Integer overflow in Google Chrome before 31.0.1650.57 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as demonstrated during a Mobile Pwn2Own competition at PacSec 2013.
CVE-2013-6634	The OneClickSigninHelper::ShowInfoBarIfPossible function in browser/ui/sync/one_click_signin_helper.cc in Google Chrome before 31.0.1650.63 uses an incorrect URL during realm validation, which allows remote attackers to conduct session fixation attacks and hijack web sessions by triggering improper sync after a 302 (aka Found) HTTP status code.

CVE-2013-6635	Use-after-free vulnerability in the editing implementation in Blink, as used in Google Chrome before 31.0.1650.63, allows remote attackers to cause a denial of service or possibly have unspecified other impact via JavaScript code that triggers removal of a node during processing of the DOM tree, related to CompositeEditCommand.cpp and ReplaceSelectionCommand.cpp.
CVE-2013-6636	The FrameLoader::notifyIfInitialDocumentAccessed function in core/loader/FrameLoader.cpp in Blink, as used in Google Chrome before 31.0.1650.63, makes an incorrect check for an empty document during presentation of a modal dialog, which allows remote attackers to spoof the address bar via vectors involving the document.write method.
CVE-2013-6637	Multiple unspecified vulnerabilities in Google Chrome before 31.0.1650.63 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-6638	Multiple buffer overflows in runtime.cc in Google V8 before 3.22.24.7, as used in Google Chrome before 31.0.1650.63, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a large typed array, related to the (1) Runtime_TypedArrayInitialize and (2) Runtime_TypedArrayInitializeFromArrayLike functions.
CVE-2013-6639	The DehoistArrayIndex function in hydrogen-dehoist.cc (aka hydrogen.cc) in Google V8 before 3.22.24.7, as used in Google Chrome before 31.0.1650.63, allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via JavaScript code that sets the value of an array element with a crafted index.
CVE-2013-6640	The DehoistArrayIndex function in hydrogen-dehoist.cc (aka hydrogen.cc) in Google V8 before 3.22.24.7, as used in Google Chrome before 31.0.1650.63, allows remote attackers to cause a denial of service (out-of-bounds read) via JavaScript code that sets a variable to the value of an array element with a crafted index.
CVE-2013-6641	Use-after-free vulnerability in the FormAssociatedElement::formRemovedFromTree function in core/html/FormAssociatedElement.cpp in Blink, as used in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of the past names map of a FORM element.
CVE-2013-6643	The OneClickSigninBubbleView::WindowClosing function in browser/ui/views/sync/

	one_click_signin_bubble_view.cc in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allows attackers to trigger a sync with an arbitrary Google account by leveraging improper handling of the closing of an untrusted signin confirm dialog.
CVE-2013-6644	Multiple unspecified vulnerabilities in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-6645	Use-after-free vulnerability in the OnWindowRemovingFromRootWindow function in content/browser/web_contents/web_contents_view_aura.cc in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving certain print-preview and tab-switch actions that interact with a speech input element.
CVE-2013-6646	Use-after-free vulnerability in the Web Workers implementation in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the shutting down of a worker process.
CVE-2013-6649	Use-after-free vulnerability in the RenderSVGImage::paint function in core/rendering/svg/RenderSVGImage.cpp in Blink, as used in Google Chrome before 32.0.1700.102, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a zero-size SVG image.
CVE-2013-6650	The StoreBuffer::ExemptPopularPages function in store-buffer.cc in Google V8 before 3.22.24.16, as used in Google Chrome before 32.0.1700.102, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via vectors that trigger incorrect handling of "popular pages."
CVE-2013-6653	Use-after-free vulnerability in the web contents implementation in Google Chrome before 33.0.1750.117 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving attempted conflicting access to the color chooser.
CVE-2013-6654	The SVGAnimateElement::calculateAnimatedValue function in core/svg/SVGAnimateElement.cpp in Blink, as used in Google Chrome before 33.0.1750.117, does

	not properly handle unexpected data types, which allows remote attackers to cause a denial of service (incorrect cast) or possibly have unspecified other impact via unknown vectors.
CVE-2013-6655	Use-after-free vulnerability in Blink, as used in Google Chrome before 33.0.1750.117, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to improper handling of overflowchanged DOM events during interaction between JavaScript and layout.
CVE-2013-6656	The XSSAuditor::init function in core/html/parser/XSSAuditor.cpp in the XSS auditor in Blink, as used in Google Chrome before 33.0.1750.117, processes POST requests by using the body of a redirecting page instead of the body of a redirect target, which allows remote attackers to obtain sensitive information via unspecified vectors.
CVE-2013-6657	core/html/parser/XSSAuditor.cpp in the XSS auditor in Blink, as used in Google Chrome before 33.0.1750.117, inserts the about:blank URL during certain blocking of FORM elements within HTTP requests, which allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via unspecified vectors.
CVE-2013-6658	Multiple use-after-free vulnerabilities in the layout implementation in Blink, as used in Google Chrome before 33.0.1750.117, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving (1) running JavaScript code during execution of the updateWidgetPositions function or (2) making a call into a plugin during execution of the updateWidgetPositions function.
CVE-2013-6659	The SSLClientSocketNSS::Core::OwnAuthCertHandler function in net/socket/ssl_client_socket_nss.cc in Google Chrome before 33.0.1750.117 does not prevent changes to server X.509 certificates during renegotiations, which allows remote SSL servers to trigger use of a new certificate chain, inconsistent with the user's expectations, by initiating a TLS renegotiation.
CVE-2013-6660	The drag-and-drop implementation in Google Chrome before 33.0.1750.117 does not properly restrict the information in WebDropData data structures, which allows remote attackers to discover full pathnames via a crafted web site.
CVE-2013-6661	Multiple unspecified vulnerabilities in Google Chrome before 33.0.1750.117 allow attackers to bypass the sandbox protection mechanism after obtaining renderer access, or have other impact, via unknown vectors.
CVE-2013-6663	Use-after-free vulnerability in the SVGImage::setContainerSize function in core/svg/

	graphics/SVGImage.cpp in the SVG implementation in Blink, as used in Google Chrome before 33.0.1750.146, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the resizing of a view.
CVE-2013-6664	Use-after-free vulnerability in the FormAssociatedElement::formRemovedFromTree function in core/html/FormAssociatedElement.cpp in Blink, as used in Google Chrome before 33.0.1750.146, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving FORM elements, as demonstrated by use of the speech-recognition feature.
CVE-2013-6665	Heap-based buffer overflow in the ResourceProvider::InitializeSoftware function in cc/resources/resource_provider.cc in Google Chrome before 33.0.1750.146 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large texture size that triggers improper memory allocation in the software renderer.
CVE-2013-6666	The PepperFlashRendererHost::OnNavigate function in renderer/pepper/pepper_flash_renderer_host.cc in Google Chrome before 33.0.1750.146 does not verify that all headers are Cross-Origin Resource Sharing (CORS) simple headers before proceeding with a PPB_Flash.Navigate operation, which might allow remote attackers to bypass intended CORS restrictions via an inappropriate header.
CVE-2013-6667	Multiple unspecified vulnerabilities in Google Chrome before 33.0.1750.146 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-6668	Multiple unspecified vulnerabilities in Google V8 before 3.24.35.10, as used in Google Chrome before 33.0.1750.146, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-6802	Google Chrome before 31.0.1650.57 allows remote attackers to bypass intended sandbox restrictions by leveraging access to a renderer process, as demonstrated during a Mobile Pwn2Own competition at PacSec 2013, a different vulnerability than CVE-2013-6632.
CVE-2013-6886	RealVNC VNC 5.0.6 on Mac OS X, Linux, and UNIX allows local users to gain privileges via a crafted argument to the (1) vncserver, (2) vncserver-x11, or (3) Xvnc helper.
CVE-2014-0491	Adobe Flash Player before 11.7.700.260 and 11.8.x and 11.9.x before 12.0.0.38 on Windows and Mac OS X and before 11.2.202.335 on Linux, Adobe AIR before

	4.0.0.1390, Adobe AIR SDK before 4.0.0.1390, and Adobe AIR SDK & Compiler before 4.0.0.1390 allow attackers to bypass unspecified protection mechanisms via unknown vectors.
CVE-2014-0492	Adobe Flash Player before 11.7.700.260 and 11.8.x and 11.9.x before 12.0.0.38 on Windows and Mac OS X and before 11.2.202.335 on Linux, Adobe AIR before 4.0.0.1390, Adobe AIR SDK before 4.0.0.1390, and Adobe AIR SDK & Compiler before 4.0.0.1390 allow attackers to defeat the ASLR protection mechanism by leveraging an "address leak."
CVE-2014-0497	Integer underflow in Adobe Flash Player before 11.7.700.261 and 11.8.x through 12.0.x before 12.0.0.44 on Windows and Mac OS X, and before 11.2.202.336 on Linux, allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2014-0498	Stack-based buffer overflow in Adobe Flash Player before 11.7.700.269 and 11.8.x through 12.0.x before 12.0.0.70 on Windows and Mac OS X and before 11.2.202.341 on Linux, Adobe AIR before 4.0.0.1628 on Android, Adobe AIR SDK before 4.0.0.1628, and Adobe AIR SDK & Compiler before 4.0.0.1628 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2014-0499	Adobe Flash Player before 11.7.700.269 and 11.8.x through 12.0.x before 12.0.0.70 on Windows and Mac OS X and before 11.2.202.341 on Linux, Adobe AIR before 4.0.0.1628 on Android, Adobe AIR SDK before 4.0.0.1628, and Adobe AIR SDK & Compiler before 4.0.0.1628 do not prevent access to address information, which makes it easier for attackers to bypass the ASLR protection mechanism via unspecified vectors.
CVE-2014-0502	Double free vulnerability in Adobe Flash Player before 11.7.700.269 and 11.8.x through 12.0.x before 12.0.0.70 on Windows and Mac OS X and before 11.2.202.341 on Linux, Adobe AIR before 4.0.0.1628 on Android, Adobe AIR SDK before 4.0.0.1628, and Adobe AIR SDK & Compiler before 4.0.0.1628 allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in February 2014.
CVE-2014-0503	Adobe Flash Player before 11.7.700.272 and 11.8.x through 12.0.x before 12.0.0.77 on Windows and OS X, and before 11.2.202.346 on Linux, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2014-0504	Adobe Flash Player before 11.7.700.272 and 11.8.x through 12.0.x before 12.0.0.77 on Windows and OS X, and before 11.2.202.346 on Linux, allows attackers to read the clipboard via unspecified vectors.

CVE-2014-0506	Use-after-free vulnerability in Adobe Flash Player before 11.7.700.275 and 11.8.x through 13.0.x before 13.0.0.182 on Windows and OS X and before 11.2.202.350 on Linux, Adobe AIR before 13.0.0.83 on Android, Adobe AIR SDK before 13.0.0.83, and Adobe AIR SDK & Compiler before 13.0.0.83 allows remote attackers to execute arbitrary code, and possibly bypass an Internet Explorer sandbox protection mechanism, via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2014.
CVE-2014-0507	Buffer overflow in Adobe Flash Player before 11.7.700.275 and 11.8.x through 13.0.x before 13.0.0.182 on Windows and OS X and before 11.2.202.350 on Linux, Adobe AIR before 13.0.0.83 on Android, Adobe AIR SDK before 13.0.0.83, and Adobe AIR SDK & Compiler before 13.0.0.83 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2014-0508	Adobe Flash Player before 11.7.700.275 and 11.8.x through 13.0.x before 13.0.0.182 on Windows and OS X and before 11.2.202.350 on Linux, Adobe AIR before 13.0.0.83 on Android, Adobe AIR SDK before 13.0.0.83, and Adobe AIR SDK & Compiler before 13.0.0.83 allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors.
CVE-2014-0509	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 11.7.700.275 and 11.8.x through 13.0.x before 13.0.0.182 on Windows and OS X and before 11.2.202.350 on Linux, Adobe AIR before 13.0.0.83 on Android, Adobe AIR SDK before 13.0.0.83, and Adobe AIR SDK & Compiler before 13.0.0.83 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2014-0515	Buffer overflow in Adobe Flash Player before 11.7.700.279 and 11.8.x through 13.0.x before 13.0.0.206 on Windows and OS X, and before 11.2.202.356 on Linux, allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in April 2014.
CVE-2014-0516	Adobe Flash Player before 13.0.0.214 on Windows and OS X and before 11.2.202.359 on Linux, Adobe AIR SDK before 13.0.0.111, and Adobe AIR SDK & Compiler before 13.0.0.111 allow remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2014-0517	Adobe Flash Player before 13.0.0.214 on Windows and OS X and before 11.2.202.359 on Linux, Adobe AIR SDK before 13.0.0.111, and Adobe AIR SDK & Compiler before 13.0.0.111 allow attackers to bypass intended access restrictions via unspecified

	vectors, a different vulnerability than CVE-2014-0518, CVE-2014-0519, and CVE-2014-0520.
CVE-2014-0518	Adobe Flash Player before 13.0.0.214 on Windows and OS X and before 11.2.202.359 on Linux, Adobe AIR SDK before 13.0.0.111, and Adobe AIR SDK & Compiler before 13.0.0.111 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0517, CVE-2014-0519, and CVE-2014-0520.
CVE-2014-0519	Adobe Flash Player before 13.0.0.214 on Windows and OS X and before 11.2.202.359 on Linux, Adobe AIR SDK before 13.0.0.111, and Adobe AIR SDK & Compiler before 13.0.0.111 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0517, CVE-2014-0518, and CVE-2014-0520.
CVE-2014-0520	Adobe Flash Player before 13.0.0.214 on Windows and OS X and before 11.2.202.359 on Linux, Adobe AIR SDK before 13.0.0.111, and Adobe AIR SDK & Compiler before 13.0.0.111 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0517, CVE-2014-0518, and CVE-2014-0519.
CVE-2014-0531	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2014-0532 and CVE-2014-0533.
CVE-2014-0532	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2014-0531 and CVE-2014-0533.
CVE-2014-0533	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2014-0531 and CVE-2014-0532.
CVE-2014-0534	Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR

	SDK & Compiler before 14.0.0.110 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0535.
CVE-2014-0535	Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0534.
CVE-2014-0536	Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2014-0537	Adobe Flash Player before 13.0.0.231 and 14.x before 14.0.0.145 on Windows and OS X and before 11.2.202.394 on Linux, Adobe AIR before 14.0.0.137 on Android, Adobe AIR SDK before 14.0.0.137, and Adobe AIR SDK & Compiler before 14.0.0.137 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0539.
CVE-2014-0538	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2014-0539	Adobe Flash Player before 13.0.0.231 and 14.x before 14.0.0.145 on Windows and OS X and before 11.2.202.394 on Linux, Adobe AIR before 14.0.0.137 on Android, Adobe AIR SDK before 14.0.0.137, and Adobe AIR SDK & Compiler before 14.0.0.137 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0537.
CVE-2014-0540	Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors, a different vulnerability than CVE-2014-0542, CVE-2014-0543, CVE-2014-0544, and CVE-2014-0545.

CVE-2014-0541	Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 allow attackers to bypass intended access restrictions via unspecified vectors.
CVE-2014-0542	Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors, a different vulnerability than CVE-2014-0540, CVE-2014-0543, CVE-2014-0544, and CVE-2014-0545.
CVE-2014-0543	Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors, a different vulnerability than CVE-2014-0540, CVE-2014-0542, CVE-2014-0544, and CVE-2014-0545.
CVE-2014-0544	Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors, a different vulnerability than CVE-2014-0540, CVE-2014-0542, CVE-2014-0543, and CVE-2014-0545.
CVE-2014-0545	Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors, a different vulnerability than

	CVE-2014-0540, CVE-2014-0542, CVE-2014-0543, and CVE-2014-0544.
CVE-2014-0547	Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0549, CVE-2014-0550, CVE-2014-0551, CVE-2014-0552, and CVE-2014-0555.
CVE-2014-0548	Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allow remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2014-0549	Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0547, CVE-2014-0550, CVE-2014-0551, CVE-2014-0552, and CVE-2014-0555.
CVE-2014-0550	Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0547, CVE-2014-0549, CVE-2014-0551, CVE-2014-0552, and CVE-2014-0555.
CVE-2014-0551	Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allow attackers to execute arbitrary code or cause a denial of service (memory corruption)

	via unspecified vectors, a different vulnerability than CVE-2014-0547, CVE-2014-0549, CVE-2014-0550, CVE-2014-0552, and CVE-2014-0555.
CVE-2014-0552	Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0547, CVE-2014-0549, CVE-2014-0550, CVE-2014-0551, and CVE-2014-0555.
CVE-2014-0553	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2014-0554	Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allow attackers to bypass intended access restrictions via unspecified vectors.
CVE-2014-0555	Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0547, CVE-2014-0549, CVE-2014-0550, CVE-2014-0551, and CVE-2014-0552.
CVE-2014-0556	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-0559.

CVE-2014-0557	Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors.
CVE-2014-0558	Adobe Flash Player before 13.0.0.250 and 14.x and 15.x before 15.0.0.189 on Windows and OS X and before 11.2.202.411 on Linux, Adobe AIR before 15.0.0.293, Adobe AIR SDK before 15.0.0.302, and Adobe AIR SDK & Compiler before 15.0.0.302 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0564.
CVE-2014-0559	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-0556.
CVE-2014-0564	Adobe Flash Player before 13.0.0.250 and 14.x and 15.x before 15.0.0.189 on Windows and OS X and before 11.2.202.411 on Linux, Adobe AIR before 15.0.0.293, Adobe AIR SDK before 15.0.0.302, and Adobe AIR SDK & Compiler before 15.0.0.302 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0558.
CVE-2014-0569	Integer overflow in Adobe Flash Player before 13.0.0.250 and 14.x and 15.x before 15.0.0.189 on Windows and OS X and before 11.2.202.411 on Linux, Adobe AIR before 15.0.0.293, Adobe AIR SDK before 15.0.0.302, and Adobe AIR SDK & Compiler before 15.0.0.302 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2014-0573	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-0588 and CVE-2014-8438.
CVE-2014-0574	Double free vulnerability in Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on

	Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2014-0576	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0581, CVE-2014-8440, and CVE-2014-8441.
CVE-2014-0577	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2014-0584, CVE-2014-0585, CVE-2014-0586, and CVE-2014-0590.
CVE-2014-0578	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-3115, CVE-2015-3116, CVE-2015-3125, and CVE-2015-5116.
CVE-2014-0580	Adobe Flash Player before 13.0.0.259 and 14.x through 16.x before 16.0.0.235 on Windows and OS X and before 11.2.202.425 on Linux allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2014-0581	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0576, CVE-2014-8440, and CVE-2014-8441.
CVE-2014-0582	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler

	before 15.0.0.356 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-0589.
CVE-2014-0583	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allows attackers to complete a transition from Low Integrity to Medium Integrity via unspecified vectors.
CVE-2014-0584	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2014-0577, CVE-2014-0585, CVE-2014-0586, and CVE-2014-0590.
CVE-2014-0585	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2014-0577, CVE-2014-0584, CVE-2014-0586, and CVE-2014-0590.
CVE-2014-0586	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2014-0577, CVE-2014-0584, CVE-2014-0585, and CVE-2014-0590.
CVE-2014-0587	Adobe Flash Player before 13.0.0.259 and 14.x through 16.x before 16.0.0.235 on Windows and OS X and before 11.2.202.425 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-9164.
CVE-2014-0588	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allows attackers to execute arbitrary

	code via unspecified vectors, a different vulnerability than CVE-2014-0573 and CVE-2014-8438.
CVE-2014-0589	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-0582.
CVE-2014-0590	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2014-0577, CVE-2014-0584, CVE-2014-0585, and CVE-2014-0586.
CVE-2014-1681	Multiple unspecified vulnerabilities in Google Chrome before 32.0.1700.102 have unknown impact and attack vectors, related to 12 "security fixes [that were not] either contributed by external researchers or particularly interesting."
CVE-2014-1700	Use-after-free vulnerability in modules/speech/SpeechSynthesis.cpp in Blink, as used in Google Chrome before 33.0.1750.149, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of a certain utterance data structure.
CVE-2014-1701	The GenerateFunction function in bindings/scripts/code_generator_v8.pm in Blink, as used in Google Chrome before 33.0.1750.149, does not implement a certain cross-origin restriction for the EventTarget::dispatchEvent function, which allows remote attackers to conduct Universal XSS (UXSS) attacks via vectors involving events.
CVE-2014-1702	Use-after-free vulnerability in the DatabaseThread::cleanupDatabaseThread function in modules/webdatabase/DatabaseThread.cpp in the web database implementation in Blink, as used in Google Chrome before 33.0.1750.149, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of scheduled tasks during shutdown of a thread.
CVE-2014-1703	Use-after-free vulnerability in the WebSocketDispatcherHost::SendOrDrop function in content/browser/renderer_host/websocket_dispatcher_host.cc in the Web Sockets implementation in Google Chrome before

	33.0.1750.149 might allow remote attackers to bypass the sandbox protection mechanism by leveraging an incorrect deletion in a certain failure case.
CVE-2014-1704	Multiple unspecified vulnerabilities in Google V8 before 3.23.17.18, as used in Google Chrome before 33.0.1750.149, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-1705	Google V8, as used in Google Chrome before 33.0.1750.152 on OS X and Linux and before 33.0.1750.154 on Windows, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2014-1713	Use-after-free vulnerability in the AttributeSetter function in bindings/templates/attributes.cpp in the bindings in Blink, as used in Google Chrome before 33.0.1750.152 on OS X and Linux and before 33.0.1750.154 on Windows, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the document.location value.
CVE-2014-1714	The ScopedClipboardWriter::WritePickledData function in ui/base/clipboard/scoped_clipboard_writer.cc in Google Chrome before 33.0.1750.152 on OS X and Linux and before 33.0.1750.154 on Windows does not verify a certain format value, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the clipboard.
CVE-2014-1715	Directory traversal vulnerability in Google Chrome before 33.0.1750.152 on OS X and Linux and before 33.0.1750.154 on Windows has unspecified impact and attack vectors.
CVE-2014-1716	Cross-site scripting (XSS) vulnerability in the Runtime_SetPrototype function in runtime.cc in Google V8, as used in Google Chrome before 34.0.1847.116, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, aka "Universal XSS (UXSS)."
CVE-2014-1717	Google V8, as used in Google Chrome before 34.0.1847.116, does not properly use numeric casts during handling of typed arrays, which allows remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2014-1718	Integer overflow in the SoftwareFrameManager::SwapToNewFrame function in content/browser/renderer_host/software_frame_manager.cc in the software compositor

	in Google Chrome before 34.0.1847.116 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted mapping of a large amount of renderer memory.
CVE-2014-1719	Use-after-free vulnerability in the WebSharedWorkerStub::OnTerminateWorkerContext function in content/worker/websharedworker_stub.cc in the Web Workers implementation in Google Chrome before 34.0.1847.116 allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via vectors that trigger a SharedWorker termination during script loading.
CVE-2014-1720	Use-after-free vulnerability in the HTMLBodyElement::insertedInto function in core/html/HTMLBodyElement.cpp in Blink, as used in Google Chrome before 34.0.1847.116, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving attributes.
CVE-2014-1721	Google V8, as used in Google Chrome before 34.0.1847.116, does not properly implement lazy deoptimization, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code, as demonstrated by improper handling of a heap allocation of a number outside the Small Integer (aka smi) range.
CVE-2014-1722	Use-after-free vulnerability in the RenderBlock::addChildIgnoringAnonymousColumnBlocks function in core/rendering/RenderBlock.cpp in Blink, as used in Google Chrome before 34.0.1847.116, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving addition of a child node.
CVE-2014-1723	The UnescapeURLWithOffsetsImpl function in net/base/escape.cc in Google Chrome before 34.0.1847.116 does not properly handle bidirectional Internationalized Resource Identifiers (IRIs), which makes it easier for remote attackers to spoof URLs via crafted use of right-to-left (RTL) Unicode text.
CVE-2014-1724	Use-after-free vulnerability in Free(b)soft Laboratory Speech Dispatcher 0.7.1, as used in Google Chrome before 34.0.1847.116, allows remote attackers to cause a denial of service (application hang) or possibly have unspecified other impact via a text-to-speech request.
CVE-2014-1725	The base64DecodeInternal function in wtf/text/Base64.cpp in Blink, as used in Google Chrome before 34.0.1847.116, does not properly handle string data composed exclusively of whitespace characters, which

	allows remote attackers to cause a denial of service (out-of-bounds read) via a window.atob method call.
CVE-2014-1726	The drag implementation in Google Chrome before 34.0.1847.116 allows user-assisted remote attackers to bypass the Same Origin Policy and forge local pathnames by leveraging renderer access.
CVE-2014-1727	Use-after-free vulnerability in content/renderer/renderer_webcolorchooser_impl.h in Google Chrome before 34.0.1847.116 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to forms.
CVE-2014-1728	Multiple unspecified vulnerabilities in Google Chrome before 34.0.1847.116 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-1729	Multiple unspecified vulnerabilities in Google V8 before 3.24.35.22, as used in Google Chrome before 34.0.1847.116, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-1730	Google V8, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, does not properly store internationalization metadata, which allows remote attackers to bypass intended access restrictions by leveraging "type confusion" and reading property values, related to i18n.js and runtime.cc.
CVE-2014-1731	core/html/HTMLSelectElement.cpp in the DOM implementation in Blink, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, does not properly check renderer state upon a focus event, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion" for SELECT elements.
CVE-2014-1732	Use-after-free vulnerability in browser/ui/views/speech_recognition_bubble_views.cc in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact via an INPUT element that triggers the presence of a Speech Recognition Bubble window for an incorrect duration.
CVE-2014-1733	The PointerCompare function in codegen.cc in Seccomp-BPF, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, does not properly merge blocks, which might allow remote attackers to bypass intended sandbox restrictions by leveraging renderer access.

CVE-2014-1734	Multiple unspecified vulnerabilities in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-1735	Multiple unspecified vulnerabilities in Google V8 before 3.24.35.33, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-1736	Integer overflow in api.cc in Google V8, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large length value.
CVE-2014-1740	Multiple use-after-free vulnerabilities in net/websockets/websocket_job.cc in the WebSockets implementation in Google Chrome before 34.0.1847.137 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to WebSocketJob deletion.
CVE-2014-1741	Multiple integer overflows in the replace-data functionality in the CharacterData interface implementation in core/dom/CharacterData.cpp in Blink, as used in Google Chrome before 34.0.1847.137, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to ranges.
CVE-2014-1742	Use-after-free vulnerability in the FrameSelection::updateAppearance function in core/editing/FrameSelection.cpp in Blink, as used in Google Chrome before 34.0.1847.137, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper RenderObject handling.
CVE-2014-1743	Use-after-free vulnerability in the StyleElement::removedFromDocument function in core/dom/StyleElement.cpp in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code that triggers tree mutation.
CVE-2014-1744	Integer overflow in the AudioInputRendererHost::OnCreateStream function in content/browser/renderer_host/media/audio_input_renderer_host.cc in Google Chrome before 35.0.1916.114 allows remote attackers to cause a denial of service or possibly have unspecified other

	impact via vectors that trigger a large shared-memory allocation.
CVE-2014-1745	Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger removal of an SVGFontFaceElement object, related to core/svg/SVGFontFaceElement.cpp.
CVE-2014-1746	The InMemoryUrlProtocol::Read function in media/filters/in_memory_url_protocol.cc in Google Chrome before 35.0.1916.114 relies on an insufficiently large integer data type, which allows remote attackers to cause a denial of service (out-of-bounds read) via vectors that trigger use of a large buffer.
CVE-2014-1747	Cross-site scripting (XSS) vulnerability in the DocumentLoader::maybeCreateArchive function in core/loader/DocumentLoader.cpp in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to inject arbitrary web script or HTML via crafted MHTML content, aka "Universal XSS (UXSS)."
CVE-2014-1748	The ScrollView::paint function in platform/scroll/ScrollView.cpp in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to spoof the UI by extending scrollbar painting into the parent frame.
CVE-2014-1749	Multiple unspecified vulnerabilities in Google Chrome before 35.0.1916.114 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3120	The default configuration in Elasticsearch before 1.2 enables dynamic scripting, which allows remote attackers to execute arbitrary MVEL expressions and Java code via the source parameter to _search. NOTE: this only violates the vendor's intended security policy if the user does not run Elasticsearch in its own independent virtual machine.
CVE-2014-3152	Integer underflow in the LCodeGen::PrepareKeyedOperand function in arm/lithium-codegen-arm.cc in Google V8 before 3.25.28.16, as used in Google Chrome before 35.0.1916.114, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a negative key value.
CVE-2014-3154	Use-after-free vulnerability in the ChildThread::Shutdown function in content/child/child_thread.cc in the filesystem API in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to a Blink shutdown.

CVE-2014-3155	net/spdy/spdy_write_queue.cc in the SPDY implementation in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service (out-of-bounds read) by leveraging incorrect queue maintenance.
CVE-2014-3156	Buffer overflow in the clipboard implementation in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger unexpected bitmap data, related to content/renderer/renderer_clipboard_client.cc and content/renderer/webclipboard_impl.cc.
CVE-2014-3157	Heap-based buffer overflow in the FFmpegVideoDecoder::GetVideoBuffer function in media/filters/ffmpeg_video_decoder.cc in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging VideoFrame data structures that are too small for proper interaction with an underlying FFmpeg library.
CVE-2014-3160	The ResourceFetcher::canRequest function in core/fetch/ResourceFetcher.cpp in Blink, as used in Google Chrome before 36.0.1985.125, does not properly restrict subresource requests associated with SVG files, which allows remote attackers to bypass the Same Origin Policy via a crafted file.
CVE-2014-3162	Multiple unspecified vulnerabilities in Google Chrome before 36.0.1985.125 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3165	Use-after-free vulnerability in modules/websockets/WorkerThreadableWebSocketChannel.cpp in the Web Sockets implementation in Blink, as used in Google Chrome before 36.0.1985.143, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an unexpectedly long lifetime of a temporary object during method completion.
CVE-2014-3166	The Public Key Pinning (PKP) implementation in Google Chrome before 36.0.1985.143 on Windows, OS X, and Linux, and before 36.0.1985.135 on Android, does not correctly consider the properties of SPDY connections, which allows remote attackers to obtain sensitive information by leveraging the use of multiple domain names.
CVE-2014-3167	Multiple unspecified vulnerabilities in Google Chrome before 36.0.1985.143 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.

CVE-2014-3168	Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before 37.0.2062.94, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper caching associated with animation.
CVE-2014-3169	Use-after-free vulnerability in core/dom/ContainerNode.cpp in the DOM implementation in Blink, as used in Google Chrome before 37.0.2062.94, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging script execution that occurs before notification of node removal.
CVE-2014-3170	extensions/common/url_pattern.cc in Google Chrome before 37.0.2062.94 does not prevent use of a '\0' character in a host name, which allows remote attackers to spoof the extension permission dialog by relying on truncation after this character.
CVE-2014-3171	Use-after-free vulnerability in the V8 bindings in Blink, as used in Google Chrome before 37.0.2062.94, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper use of HashMap add operations instead of HashMap set operations, related to bindings/core/v8/DOMWrapperMap.h and bindings/core/v8/SerializedScriptValue.cpp.
CVE-2014-3172	The Debugger extension API in browser/extensions/api/debugger/debugger_api.cc in Google Chrome before 37.0.2062.94 does not validate a tab's URL before an attach operation, which allows remote attackers to bypass intended access limitations via an extension that uses a restricted URL, as demonstrated by a chrome:// URL.
CVE-2014-3173	The WebGL implementation in Google Chrome before 37.0.2062.94 does not ensure that clear calls interact properly with the state of a draw buffer, which allows remote attackers to cause a denial of service (read of uninitialized memory) via a crafted CANVAS element, related to gpu/command_buffer/service/framebuffer_manager.cc and gpu/command_buffer/service/gles2_cmd_decoder.cc.
CVE-2014-3174	modules/webaudio/BiquadDSPKernel.cpp in the Web Audio API implementation in Blink, as used in Google Chrome before 37.0.2062.94, does not properly consider concurrent threads during attempts to update biquad filter coefficients, which allows remote attackers to cause a denial of service (read of uninitialized memory) via crafted API calls.
CVE-2014-3175	Multiple unspecified vulnerabilities in Google Chrome before 37.0.2062.94 allow attackers to cause a denial of service or possibly have other impact via unknown

	vectors, related to the load_truetype_glyph function in truetype/ttgload.c in FreeType and other functions in other components.
CVE-2014-3176	Google Chrome before 37.0.2062.94 does not properly handle the interaction of extensions, IPC, the sync API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-3177.
CVE-2014-3177	Google Chrome before 37.0.2062.94 does not properly handle the interaction of extensions, IPC, the sync API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-3176.
CVE-2014-3178	Use-after-free vulnerability in core/dom/Node.cpp in Blink, as used in Google Chrome before 37.0.2062.120, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of render-tree inconsistencies.
CVE-2014-3179	Multiple unspecified vulnerabilities in Google Chrome before 37.0.2062.120 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3188	Google Chrome before 38.0.2125.101 and Chrome OS before 38.0.2125.101 do not properly handle the interaction of IPC and Google V8, which allows remote attackers to execute arbitrary code via vectors involving JSON data, related to improper parsing of an escaped index by ParseJsonObject in json-parser.h.
CVE-2014-3189	The chrome_pdf::CopyImage function in pdf/draw_utils.cc in the PDFium component in Google Chrome before 38.0.2125.101 does not properly validate image-data dimensions, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via unknown vectors.
CVE-2014-3190	Use-after-free vulnerability in the Event::currentTarget function in core/events/Event.cpp in Blink, as used in Google Chrome before 38.0.2125.101, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code that accesses the path property of an Event object.
CVE-2014-3191	Use-after-free vulnerability in Blink, as used in Google Chrome before 38.0.2125.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers a widget-position update that improperly interacts with the render tree, related to the FrameView::updateLayoutAndStyleForPainting function in core/frame/FrameView.cpp and the

	RenderLayerScrollableArea::setScrollOffset function in core/rendering/RenderLayerScrollableArea.cpp.
CVE-2014-3192	Use-after-free vulnerability in the ProcessingInstruction::setXSLStyleSheet function in core/dom/ProcessingInstruction.cpp in the DOM implementation in Blink, as used in Google Chrome before 38.0.2125.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-3193	The SessionService::GetLastSession function in browser/sessions/session_service.cc in Google Chrome before 38.0.2125.101 allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors that leverage "type confusion" for callback processing.
CVE-2014-3194	Use-after-free vulnerability in the Web Workers implementation in Google Chrome before 38.0.2125.101 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-3195	Google V8, as used in Google Chrome before 38.0.2125.101, does not properly track JavaScript heap-memory allocations as allocations of uninitialized memory and does not properly concatenate arrays of double-precision floating-point numbers, which allows remote attackers to obtain sensitive information via crafted JavaScript code, related to the PagedSpace::AllocateRaw and NewSpace::AllocateRaw functions in heap/spaces-inl.h, the LargeObjectSpace::AllocateRaw function in heap/spaces.cc, and the Runtime_ArrayConcat function in runtime.cc.
CVE-2014-3196	base/memory/shared_memory_win.cc in Google Chrome before 38.0.2125.101 on Windows does not properly implement read-only restrictions on shared memory, which allows attackers to bypass a sandbox protection mechanism via unspecified vectors.
CVE-2014-3197	The NavigationScheduler::schedulePageBlock function in core/loader/NavigationScheduler.cpp in Blink, as used in Google Chrome before 38.0.2125.101, does not properly provide substitute data for pages blocked by the XSS auditor, which allows remote attackers to obtain sensitive information via a crafted web site.
CVE-2014-3198	The Instance::HandleInputEvent function in pdf/instance.cc in the PDFium component in Google Chrome before 38.0.2125.101 interprets a certain -1 value as an index instead of a no-visible-page error code, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.

CVE-2014-3199	The wrap function in bindings/core/v8/custom/V8EventCustom.cpp in the V8 bindings in Blink, as used in Google Chrome before 38.0.2125.101, has an erroneous fallback outcome for wrapper-selection failures, which allows remote attackers to cause a denial of service via vectors that trigger stopping a worker process that had been handling an Event object.
CVE-2014-3200	Multiple unspecified vulnerabilities in Google Chrome before 38.0.2125.101 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3803	The SpeechInput feature in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to enable microphone access and obtain speech-recognition text without indication via an INPUT element with a -x-webkit-speech attribute.
CVE-2014-4671	Adobe Flash Player before 13.0.0.231 and 14.x before 14.0.0.145 on Windows and OS X and before 11.2.202.394 on Linux, Adobe AIR before 14.0.0.137 on Android, Adobe AIR SDK before 14.0.0.137, and Adobe AIR SDK & Compiler before 14.0.0.137 do not properly restrict the SWF file format, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks against JSONP endpoints, and obtain sensitive information, via a crafted OBJECT element with SWF content satisfying the character-set requirements of a callback API.
CVE-2014-5333	Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 do not properly restrict the SWF file format, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks against JSONP endpoints, and obtain sensitive information, via a crafted OBJECT element with SWF content satisfying the character-set requirements of a callback API, in conjunction with a manipulation involving a '$' (dollar sign) or '(' (open parenthesis) character. NOTE: this issue exists because of an incomplete fix for CVE-2014-4671.
CVE-2014-6053	The rfbProcessClientNormalMessage function in libvncserver/rfbserver.c in LibVNCServer 0.9.9 and earlier does not properly handle attempts to send a large amount of ClientCutText data, which allows remote attackers to cause a denial of service (memory consumption or daemon crash) via a crafted message that is processed by using a single unchecked malloc.
CVE-2014-7899	Google Chrome before 38.0.2125.101 allows remote attackers to spoof the address bar by placing a blob:

	substring at the beginning of the URL, followed by the original URI scheme and a long username string.
CVE-2014-7900	Use-after-free vulnerability in the CPDF_Parser::IsLinearizedFile function in fpdfapi/fpdf_parser/fpdf_parser_parser.cpp in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.
CVE-2014-7901	Integer overflow in the opj_t2_read_packet_data function in fxcodec/fx_libopenjpeg/libopenjpeg20/t2.c in OpenJPEG in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long segment in a JPEG image.
CVE-2014-7902	Use-after-free vulnerability in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.
CVE-2014-7903	Buffer overflow in OpenJPEG before r2911 in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted JPEG image.
CVE-2014-7904	Buffer overflow in Skia, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-7906	Use-after-free vulnerability in the Pepper plugins in Google Chrome before 39.0.2171.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted Flash content that triggers an attempted PepperMediaDeviceManager access outside of the object's lifetime.
CVE-2014-7907	Multiple use-after-free vulnerabilities in modules/screen_orientation/ScreenOrientationController.cpp in Blink, as used in Google Chrome before 39.0.2171.65, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger improper handling of a detached frame, related to the (1) lock and (2) unlock methods.
CVE-2014-7908	Multiple integer overflows in the CheckMov function in media/base/container_names.cc in Google Chrome before 39.0.2171.65 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a large atom in (1) MPEG-4 or (2) QuickTime .mov data.
CVE-2014-7909	effects/SkDashPathEffect.cpp in Skia, as used in Google Chrome before 39.0.2171.65, computes a hash key using uninitialized integer values, which might

	allow remote attackers to cause a denial of service by rendering crafted data.
CVE-2014-7910	Multiple unspecified vulnerabilities in Google Chrome before 39.0.2171.65 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-7923	The Regular Expressions package in International Components for Unicode (ICU) 52 before SVN revision 292944, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via vectors related to a look-behind expression.
CVE-2014-7924	Use-after-free vulnerability in the IndexedDB implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering duplicate BLOB references, related to content/browser/indexed_db/indexed_db_callbacks.cc and content/browser/indexed_db/indexed_db_dispatcher_host.cc.
CVE-2014-7925	Use-after-free vulnerability in the WebAudio implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an audio-rendering thread in which AudioNode data is improperly maintained.
CVE-2014-7926	The Regular Expressions package in International Components for Unicode (ICU) 52 before SVN revision 292944, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via vectors related to a zero-length quantifier.
CVE-2014-7927	The SimplifiedLowering::DoLoadBuffer function in compiler/simplified-lowering.cc in Google V8, as used in Google Chrome before 40.0.2214.91, does not properly choose an integer data type, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2014-7928	hydrogen.cc in Google V8, as used Google Chrome before 40.0.2214.91, does not properly handle arrays with holes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code that triggers an array copy.
CVE-2014-7929	Use-after-free vulnerability in the HTMLScriptElement::didMoveToNewDocument function in core/html/HTMLScriptElement.cpp in the DOM

	implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving movement of a SCRIPT element across documents.
CVE-2014-7930	Use-after-free vulnerability in core/events/TreeScopeEventContext.cpp in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers improper maintenance of TreeScope data.
CVE-2014-7931	factory.cc in Google V8, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code that triggers improper maintenance of backing-store pointers.
CVE-2014-7932	Use-after-free vulnerability in the Element::detach function in core/dom/Element.cpp in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving pending updates of detached elements.
CVE-2014-7933	Use-after-free vulnerability in the matroska_read_seek function in libavformat/matroskadec.c in FFmpeg before 2.5.1, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Matroska file that triggers improper maintenance of tracks data.
CVE-2014-7934	Use-after-free vulnerability in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to unexpected absence of document data structures.
CVE-2014-7935	Use-after-free vulnerability in browser/speech/tts_message_filter.cc in the Speech implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving utterances from a closed tab.
CVE-2014-7936	Use-after-free vulnerability in the ZoomBubbleView::Close function in browser/ui/views/location_bar/zoom_bubble_view.cc in the Views implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted

	document that triggers improper maintenance of a zoom bubble.
CVE-2014-7937	Multiple off-by-one errors in libavcodec/vorbisdec.c in FFmpeg before 2.4.2, as used in Google Chrome before 40.0.2214.91, allow remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted Vorbis I data.
CVE-2014-7938	The Fonts implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2014-7939	Google Chrome before 40.0.2214.91, when the Harmony proxy in Google V8 is enabled, allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code with Proxy.create and console.log calls, related to HTTP responses that lack an "X-Content-Type-Options: nosniff" header.
CVE-2014-7940	The collator implementation in i18n/ucol.cpp in International Components for Unicode (ICU) 52 through SVN revision 293126, as used in Google Chrome before 40.0.2214.91, does not initialize memory for a data structure, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted character sequence.
CVE-2014-7941	The SelectionOwner::ProcessTarget function in ui/base/x/selection_owner.cc in the UI implementation in Google Chrome before 40.0.2214.91 uses an incorrect data type for a certain length value, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted X11 data.
CVE-2014-7942	The Fonts implementation in Google Chrome before 40.0.2214.91 does not initialize memory for a data structure, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-7943	Skia, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2014-7944	The sycc422_to_rgb function in fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 40.0.2214.91, does not properly handle odd values of image width, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document.
CVE-2014-7945	OpenJPEG before r2908, as used in PDFium in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document, related to j2k.c, jp2.c, and t2.c.

CVE-2014-7946	The RenderTable::simplifiedNormalFlowLayout function in core/rendering/RenderTable.cpp in Blink, as used in Google Chrome before 40.0.2214.91, skips captions during table layout in certain situations, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors related to the Fonts implementation.
CVE-2014-7947	OpenJPEG before r2944, as used in PDFium in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document, related to j2k.c, jp2.c, pi.c, t1.c, t2.c, and tcd.c.
CVE-2014-7948	The AppCacheUpdateJob::URLFetcher::OnResponseStarted function in content/browser/appcache/appcache_update_job.cc in Google Chrome before 40.0.2214.91 proceeds with AppCache caching for SSL sessions even if there is an X.509 certificate error, which allows man-in-the-middle attackers to spoof HTML5 application content via a crafted certificate.
CVE-2014-7967	Multiple unspecified vulnerabilities in Google V8 before 3.28.71.15, as used in Google Chrome before 38.0.2125.101, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-8437	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow remote attackers to discover session tokens via unspecified vectors.
CVE-2014-8438	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-0573 and CVE-2014-0588.
CVE-2014-8439	Adobe Flash Player before 13.0.0.258 and 14.x and 15.x before 15.0.0.239 on Windows and OS X and before 11.2.202.424 on Linux, Adobe AIR before 15.0.0.293, Adobe AIR SDK before 15.0.0.302, and Adobe AIR SDK & Compiler before 15.0.0.302 allow attackers to execute arbitrary code or cause a denial of service (invalid pointer dereference) via unspecified vectors.
CVE-2014-8440	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and

	before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0576, CVE-2014-0581, and CVE-2014-8441.
CVE-2014-8441	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0576, CVE-2014-0581, and CVE-2014-8440.
CVE-2014-8442	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to complete a transition from Low Integrity to Medium Integrity by leveraging incorrect permissions.
CVE-2014-8443	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.259 and 14.x through 16.x before 16.0.0.235 on Windows and OS X and before 11.2.202.425 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2014-9162	Adobe Flash Player before 13.0.0.259 and 14.x through 16.x before 16.0.0.235 on Windows and OS X and before 11.2.202.425 on Linux allows attackers to obtain sensitive information via unspecified vectors.
CVE-2014-9163	Stack-based buffer overflow in Adobe Flash Player before 13.0.0.259 and 14.x and 15.x before 15.0.0.246 on Windows and OS X and before 11.2.202.425 on Linux allows attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in December 2014.
CVE-2014-9164	Adobe Flash Player before 13.0.0.259 and 14.x through 16.x before 16.0.0.235 on Windows and OS X and before 11.2.202.425 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0587.
CVE-2014-9646	Unquoted Windows search path vulnerability in the GoogleChromeDistribution::DoPostUninstallOperations function in installer/util/google_chrome_distribution.cc in the uninstall-survey feature in Google Chrome before 40.0.2214.91 allows local users to gain privileges via a Trojan horse program in the %SYSTEMDRIVE%

	directory, as demonstrated by program.exe, a different vulnerability than CVE-2015-1205.
CVE-2014-9647	Use-after-free vulnerability in PDFium, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document, related to fpdfsdk/src/fpdfview.cpp and fpdfsdk/src/fsdk_mgr.cpp, a different vulnerability than CVE-2015-1205.
CVE-2014-9654	The Regular Expressions package in International Components for Unicode (ICU) for C/C++ before 2014-12-03, as used in Google Chrome before 40.0.2214.91, calculates certain values without ensuring that they can be represented in a 24-bit field, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted string, a related issue to CVE-2014-7923.
CVE-2014-9689	content/renderer/device_sensors/device_orientation_event_pump.cc in Google Chrome before 41.0.2272.76 does not properly restrict access to high-rate gyroscope data, which makes it easier for remote attackers to obtain speech signals from a device's physical environment via a crafted web site that listens for ondeviceorientation events, a different vulnerability than CVE-2015-1231.
CVE-2015-0301	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 do not properly validate files, which has unspecified impact and attack vectors.
CVE-2015-0302	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allow attackers to obtain sensitive keystroke information via unspecified vectors.
CVE-2015-0303	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allow attackers to execute arbitrary code or cause a denial of service (memory corruption)

	via unspecified vectors, a different vulnerability than CVE-2015-0306.
CVE-2015-0304	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0309.
CVE-2015-0305	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion."
CVE-2015-0306	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0303.
CVE-2015-0307	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2015-0308	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-0309	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android,

	Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0304.
CVE-2015-0310	Adobe Flash Player before 13.0.0.262 and 14.x through 16.x before 16.0.0.287 on Windows and OS X and before 11.2.202.438 on Linux does not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism on Windows, and have an unspecified impact on other platforms, via unknown vectors, as exploited in the wild in January 2015.
CVE-2015-0311	Unspecified vulnerability in Adobe Flash Player through 13.0.0.262 and 14.x, 15.x, and 16.x through 16.0.0.287 on Windows and OS X and through 11.2.202.438 on Linux allows remote attackers to execute arbitrary code via unknown vectors, as exploited in the wild in January 2015.
CVE-2015-0312	Double free vulnerability in Adobe Flash Player before 13.0.0.264 and 14.x through 16.x before 16.0.0.296 on Windows and OS X and before 11.2.202.440 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-0313	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in February 2015, a different vulnerability than CVE-2015-0315, CVE-2015-0320, and CVE-2015-0322.
CVE-2015-0314	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0316, CVE-2015-0318, CVE-2015-0321, CVE-2015-0329, and CVE-2015-0330.
CVE-2015-0315	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0313, CVE-2015-0320, and CVE-2015-0322.
CVE-2015-0316	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified

	vectors, a different vulnerability than CVE-2015-0314, CVE-2015-0318, CVE-2015-0321, CVE-2015-0329, and CVE-2015-0330.
CVE-2015-0317	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-0319.
CVE-2015-0318	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0314, CVE-2015-0316, CVE-2015-0321, CVE-2015-0329, and CVE-2015-0330.
CVE-2015-0319	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-0317.
CVE-2015-0320	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0313, CVE-2015-0315, and CVE-2015-0322.
CVE-2015-0321	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0314, CVE-2015-0316, CVE-2015-0318, CVE-2015-0329, and CVE-2015-0330.
CVE-2015-0322	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0313, CVE-2015-0315, and CVE-2015-0320.
CVE-2015-0323	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute

	arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0327.
CVE-2015-0324	Buffer overflow in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-0325	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2015-0326 and CVE-2015-0328.
CVE-2015-0326	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2015-0325 and CVE-2015-0328.
CVE-2015-0327	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0323.
CVE-2015-0328	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2015-0325 and CVE-2015-0326.
CVE-2015-0329	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0314, CVE-2015-0316, CVE-2015-0318, CVE-2015-0321, and CVE-2015-0330.
CVE-2015-0330	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0314, CVE-2015-0316, CVE-2015-0318, CVE-2015-0321, and CVE-2015-0329.

CVE-2015-0331	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0313, CVE-2015-0315, CVE-2015-0320, and CVE-2015-0322.
CVE-2015-0332	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0333, CVE-2015-0335, and CVE-2015-0339.
CVE-2015-0333	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0332, CVE-2015-0335, and CVE-2015-0339.
CVE-2015-0334	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-0336.
CVE-2015-0335	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0332, CVE-2015-0333, and CVE-2015-0339.
CVE-2015-0336	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-0334.
CVE-2015-0337	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2015-0338	Integer overflow in Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code via unspecified vectors.

CVE-2015-0339	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0332, CVE-2015-0333, and CVE-2015-0335.
CVE-2015-0340	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows remote attackers to bypass intended file-upload restrictions via unspecified vectors.
CVE-2015-0341	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0342.
CVE-2015-0342	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0341.
CVE-2015-0346	Double free vulnerability in Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0359.
CVE-2015-0347	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0350, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, CVE-2015-3042, and CVE-2015-3043.
CVE-2015-0348	Buffer overflow in Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-0349	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different

	vulnerability than CVE-2015-0351, CVE-2015-0358, and CVE-2015-3039.
CVE-2015-0350	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0347, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, CVE-2015-3042, and CVE-2015-3043.
CVE-2015-0351	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0349, CVE-2015-0358, and CVE-2015-3039.
CVE-2015-0352	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0347, CVE-2015-0350, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, CVE-2015-3042, and CVE-2015-3043.
CVE-2015-0353	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0347, CVE-2015-0350, CVE-2015-0352, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, CVE-2015-3042, and CVE-2015-3043.
CVE-2015-0354	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0347, CVE-2015-0350, CVE-2015-0352, CVE-2015-0353, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, CVE-2015-3042, and CVE-2015-3043.
CVE-2015-0355	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0347, CVE-2015-0350,

	CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, CVE-2015-3042, and CVE-2015-3043.
CVE-2015-0356	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion."
CVE-2015-0357	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux does not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors, a different vulnerability than CVE-2015-3040.
CVE-2015-0358	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0349, CVE-2015-0351, and CVE-2015-3039.
CVE-2015-0359	Double free vulnerability in Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0346.
CVE-2015-0360	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0347, CVE-2015-0350, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-3038, CVE-2015-3041, CVE-2015-3042, and CVE-2015-3043.
CVE-2015-1205	Multiple unspecified vulnerabilities in Google Chrome before 40.0.2214.91 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1209	Use-after-free vulnerability in the VisibleSelection::nonBoundaryShadowTreeRootNode function in core/editing/VisibleSelection.cpp in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript

	code that triggers improper handling of a shadow-root anchor.
CVE-2015-1210	The V8ThrowException::createDOMException function in bindings/core/v8/V8ThrowException.cpp in the V8 bindings in Blink, as used in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android, does not properly consider frame access restrictions during the throwing of an exception, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2015-1211	The OriginCanAccessServiceWorkers function in content/browser/service_worker/service_worker_dispatcher_host.cc in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android does not properly restrict the URI scheme during a ServiceWorker registration, which allows remote attackers to gain privileges via a filesystem: URI.
CVE-2015-1212	Multiple unspecified vulnerabilities in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1213	The SkBitmap::ReadRawPixels function in core/SkBitmap.cpp in the filters implementation in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an out-of-bounds write operation.
CVE-2015-1214	Integer overflow in the SkAutoSTArray implementation in include/core/SkTemplates.h in the filters implementation in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a reset action with a large count value, leading to an out-of-bounds write operation.
CVE-2015-1215	The filters implementation in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an out-of-bounds write operation.
CVE-2015-1216	Use-after-free vulnerability in the V8Window::namedPropertyGetterCustom function in bindings/core/v8/custom/V8WindowCustom.cpp in the V8 bindings in Blink, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a frame detachment.

CVE-2015-1217	The V8LazyEventListener::prepareListenerObject function in bindings/core/v8/V8LazyEventListener.cpp in the V8 bindings in Blink, as used in Google Chrome before 41.0.2272.76, does not properly compile listeners, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2015-1218	Multiple use-after-free vulnerabilities in the DOM implementation in Blink, as used in Google Chrome before 41.0.2272.76, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger movement of a SCRIPT element to different documents, related to (1) the HTMLScriptElement::didMoveToNewDocument function in core/html/HTMLScriptElement.cpp and (2) the SVGScriptElement::didMoveToNewDocument function in core/svg/SVGScriptElement.cpp.
CVE-2015-1219	Integer overflow in the SkMallocPixelRef::NewAllocate function in core/SkMallocPixelRef.cpp in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted allocation of a large amount of memory during WebGL rendering.
CVE-2015-1220	Use-after-free vulnerability in the GIFImageReader::parseData function in platform/image-decoders/gif/GIFImageReader.cpp in Blink, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted frame size in a GIF image.
CVE-2015-1221	Use-after-free vulnerability in Blink, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect ordering of operations in the Web SQL Database thread relative to Blink's main thread, related to the shutdown function in web/WebKit.cpp.
CVE-2015-1222	Multiple use-after-free vulnerabilities in the ServiceWorkerScriptCacheMap implementation in content/browser/service_worker/service_worker_script_cache_map.cc in Google Chrome before 41.0.2272.76 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a ServiceWorkerContextWrapper::DeleteAndStartOver call, related to the NotifyStartedCaching and NotifyFinishedCaching functions.
CVE-2015-1223	Multiple use-after-free vulnerabilities in core/html/HTMLInputElement.cpp in the DOM implementation in Blink, as used in Google Chrome before 41.0.2272.76,

	allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger extraneous change events, as demonstrated by events for invalid input or input to read-only fields, related to the initializeTypeInParsing and updateType functions.
CVE-2015-1224	The VpxVideoDecoder::VpxDecode function in media/filters/vpx_video_decoder.cc in the vpxdecoder implementation in Google Chrome before 41.0.2272.76 does not ensure that alpha-plane dimensions are identical to image dimensions, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted VPx video data.
CVE-2015-1225	PDFium, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2015-1226	The DebuggerFunction::InitAgentHost function in browser/extensions/api/debugger/debugger_api.cc in Google Chrome before 41.0.2272.76 does not properly restrict what URLs are available as debugger targets, which allows remote attackers to bypass intended access restrictions via a crafted extension.
CVE-2015-1227	The DragImage::create function in platform/DragImage.cpp in Blink, as used in Google Chrome before 41.0.2272.76, does not initialize memory for image drawing, which allows remote attackers to have an unspecified impact by triggering a failed image decoding, as demonstrated by an image for which the default orientation cannot be used.
CVE-2015-1228	The RenderCounter::updateCounter function in core/rendering/RenderCounter.cpp in Blink, as used in Google Chrome before 41.0.2272.76, does not force a relayout operation and consequently does not initialize memory for a data structure, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted Cascading Style Sheets (CSS) token sequence.
CVE-2015-1229	net/http/proxy_client_socket.cc in Google Chrome before 41.0.2272.76 does not properly handle a 407 (aka Proxy Authentication Required) HTTP status code accompanied by a Set-Cookie header, which allows remote proxy servers to conduct cookie-injection attacks via a crafted response.
CVE-2015-1230	The getHiddenProperty function in bindings/core/v8/V8EventListenerList.h in Blink, as used in Google Chrome before 41.0.2272.76, has a name conflict with the AudioContext class, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via JavaScript code that

	adds an AudioContext event listener and triggers "type confusion."
CVE-2015-1231	Multiple unspecified vulnerabilities in Google Chrome before 41.0.2272.76 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1232	Array index error in the MidiManagerUsb::DispatchSendMidiData function in media/midi/midi_manager_usb.cc in Google Chrome before 41.0.2272.76 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging renderer access to provide an invalid port index that triggers an out-of-bounds write operation, a different vulnerability than CVE-2015-1212.
CVE-2015-1233	Google Chrome before 41.0.2272.118 does not properly handle the interaction of IPC, the Gamepad API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2015-1234	Race condition in gpu/command_buffer/service/gles2_cmd_decoder.cc in Google Chrome before 41.0.2272.118 allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact by manipulating OpenGL ES commands.
CVE-2015-1235	The ContainerNode::parserRemoveChild function in core/dom/ContainerNode.cpp in the HTML parser in Blink, as used in Google Chrome before 42.0.2311.90, allows remote attackers to bypass the Same Origin Policy via a crafted HTML document with an IFRAME element.
CVE-2015-1236	The MediaElementAudioSourceNode::process function in modules/webaudio/MediaElementAudioSourceNode.cpp in the Web Audio API implementation in Blink, as used in Google Chrome before 42.0.2311.90, allows remote attackers to bypass the Same Origin Policy and obtain sensitive audio sample values via a crafted web site containing a media element.
CVE-2015-1237	Use-after-free vulnerability in the RenderFrameImpl::OnMessageReceived function in content/renderer/render_frame_impl.cc in Google Chrome before 42.0.2311.90 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger renderer IPC messages during a detach operation.
CVE-2015-1238	Skia, as used in Google Chrome before 42.0.2311.90, allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via unknown vectors.

CVE-2015-1240	gpu/blink/webgraphicscontext3d_impl.cc in the WebGL implementation in Google Chrome before 42.0.2311.90 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WebGL program that triggers a state inconsistency.
CVE-2015-1241	Google Chrome before 42.0.2311.90 does not properly consider the interaction of page navigation with the handling of touch events and gesture events, which allows remote attackers to trigger unintended UI actions via a crafted web site that conducts a "tapjacking" attack.
CVE-2015-1242	The ReduceTransitionElementsKind function in hydrogen-check-elimination.cc in Google V8 before 4.2.77.8, as used in Google Chrome before 42.0.2311.90, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that leverages "type confusion" in the check-elimination optimization.
CVE-2015-1243	Use-after-free vulnerability in the MutationObserver::disconnect function in core/dom/MutationObserver.cpp in the DOM implementation in Blink, as used in Google Chrome before 42.0.2311.135, allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering an attempt to unregister a MutationObserver object that is not currently registered.
CVE-2015-1244	The URLRequest::GetHSTSRedirect function in url_request/url_request.cc in Google Chrome before 42.0.2311.90 does not replace the ws scheme with the wss scheme whenever an HSTS Policy is active, which makes it easier for remote attackers to obtain sensitive information by sniffing the network for WebSocket traffic.
CVE-2015-1245	Use-after-free vulnerability in the OpenPDFInReaderView::Update function in browser/ui/views/location_bar/open_pdf_in_reader_view.cc in Google Chrome before 41.0.2272.76 might allow user-assisted remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by triggering interaction with a PDFium "Open PDF in Reader" button that has an invalid tab association.
CVE-2015-1246	Blink, as used in Google Chrome before 42.0.2311.90, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2015-1247	The SearchEngineTabHelper::OnPageHasOSDD function in browser/ui/search_engines/search_engine_tab_helper.cc in Google Chrome before 42.0.2311.90 does not prevent use of a file: URL for an OpenSearch descriptor XML document, which might

	allow remote attackers to obtain sensitive information from local files via a crafted (1) http or (2) https web site.
CVE-2015-1248	The FileSystem API in Google Chrome before 40.0.2214.91 allows remote attackers to bypass the SafeBrowsing for Executable Files protection mechanism by creating a .exe file in a temporary filesystem and then referencing this file with a filesystem:http: URL.
CVE-2015-1249	Multiple unspecified vulnerabilities in Google Chrome before 42.0.2311.90 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1250	Multiple unspecified vulnerabilities in Google Chrome before 42.0.2311.135 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1251	Use-after-free vulnerability in the SpeechRecognitionClient implementation in the Speech subsystem in Google Chrome before 43.0.2357.65 allows remote attackers to execute arbitrary code via a crafted document.
CVE-2015-1252	common/partial_circular_buffer.cc in Google Chrome before 43.0.2357.65 does not properly handle wraps, which allows remote attackers to bypass a sandbox protection mechanism or cause a denial of service (out-of-bounds write) via vectors that trigger a write operation with a large amount of data, related to the PartialCircularBuffer::Write and PartialCircularBuffer::DoWrite functions.
CVE-2015-1253	core/html/parser/HTMLConstructionSite.cpp in the DOM implementation in Blink, as used in Google Chrome before 43.0.2357.65, allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code that appends a child to a SCRIPT element, related to the insert and executeReparentTask functions.
CVE-2015-1254	core/dom/Document.cpp in Blink, as used in Google Chrome before 43.0.2357.65, enables the inheritance of the designMode attribute, which allows remote attackers to bypass the Same Origin Policy by leveraging the availability of editing.
CVE-2015-1255	Use-after-free vulnerability in content/renderer/media/webaudio_capturer_source.cc in the WebAudio implementation in Google Chrome before 43.0.2357.65 allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by leveraging improper handling of a stop action for an audio track.
CVE-2015-1256	Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before

	43.0.2357.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document that leverages improper handling of a shadow tree for a use element.
CVE-2015-1257	platform/graphics/filters/FEColorMatrix.cpp in the SVG implementation in Blink, as used in Google Chrome before 43.0.2357.65, does not properly handle an insufficient number of values in an feColorMatrix filter, which allows remote attackers to cause a denial of service (container overflow) or possibly have unspecified other impact via a crafted document.
CVE-2015-1258	Google Chrome before 43.0.2357.65 relies on libvpx code that was not built with an appropriate --size-limit value, which allows remote attackers to trigger a negative value for a size field, and consequently cause a denial of service or possibly have unspecified other impact, via a crafted frame size in VP9 video data.
CVE-2015-1259	PDFium, as used in Google Chrome before 43.0.2357.65, does not properly initialize memory, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2015-1260	Multiple use-after-free vulnerabilities in content/renderer/media/user_media_client_impl.cc in the WebRTC implementation in Google Chrome before 43.0.2357.65 allow remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that executes upon completion of a getUserMedia request.
CVE-2015-1262	platform/fonts/shaping/HarfBuzzShaper.cpp in Blink, as used in Google Chrome before 43.0.2357.65, does not initialize a certain width field, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted Unicode text.
CVE-2015-1263	The Spellcheck API implementation in Google Chrome before 43.0.2357.65 does not use an HTTPS session for downloading a Hunspell dictionary, which allows man-in-the-middle attackers to deliver incorrect spelling suggestions or possibly have unspecified other impact via a crafted file.
CVE-2015-1264	Cross-site scripting (XSS) vulnerability in Google Chrome before 43.0.2357.65 allows user-assisted remote attackers to inject arbitrary web script or HTML via crafted data that is improperly handled by the Bookmarks feature.
CVE-2015-1265	Multiple unspecified vulnerabilities in Google Chrome before 43.0.2357.65 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.

CVE-2015-1266	content/browser/webui/content_web_ui_controller_factory.cc in Google Chrome before 43.0.2357.130 does not properly consider the scheme in determining whether a URL is associated with a WebUI SiteInstance, which allows remote attackers to bypass intended access restrictions via a similar URL, as demonstrated by use of http://gpu when there is a WebUI class for handling chrome://gpu requests.
CVE-2015-1267	Blink, as used in Google Chrome before 43.0.2357.130, does not properly restrict the creation context during creation of a DOM wrapper, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code that uses a Blink public API, related to WebArrayBufferConverter.cpp, WebBlob.cpp, WebDOMError.cpp, and WebDOMFileSystem.cpp.
CVE-2015-1268	bindings/scripts/v8_types.py in Blink, as used in Google Chrome before 43.0.2357.130, does not properly select a creation context for a return value's DOM wrapper, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code, as demonstrated by use of a data: URL.
CVE-2015-1269	The DecodeHSTSPreloadRaw function in net/http/transport_security_state.cc in Google Chrome before 43.0.2357.130 does not properly canonicalize DNS hostnames before making comparisons to HSTS or HPKP preload entries, which allows remote attackers to bypass intended access restrictions via a string that (1) ends in a . (dot) character or (2) is not entirely lowercase.
CVE-2015-1270	The ucnv_io_getConverterName function in common/ucnv_io.cpp in International Components for Unicode (ICU), as used in Google Chrome before 44.0.2403.89, mishandles converter names with initial x- substrings, which allows remote attackers to cause a denial of service (read of uninitialized memory) or possibly have unspecified other impact via a crafted file.
CVE-2015-1271	PDFium, as used in Google Chrome before 44.0.2403.89, does not properly handle certain out-of-memory conditions, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted PDF document that triggers a large memory allocation.
CVE-2015-1272	Use-after-free vulnerability in the GPU process implementation in Google Chrome before 44.0.2403.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging the continued availability of a GPUChannelHost data structure during Blink shutdown, related to content/browser/gpu/browser_gpu_channel_host_factory.cc and content/renderer/render_thread_impl.cc.

CVE-2015-1273	Heap-based buffer overflow in j2k.c in OpenJPEG before r3002, as used in PDFium in Google Chrome before 44.0.2403.89, allows remote attackers to cause a denial of service or possibly have unspecified other impact via invalid JPEG2000 data in a PDF document.
CVE-2015-1274	Google Chrome before 44.0.2403.89 does not ensure that the auto-open list omits all dangerous file types, which makes it easier for remote attackers to execute arbitrary code by providing a crafted file and leveraging a user's previous "Always open files of this type" choice, related to download_commands.cc and download_prefs.cc.
CVE-2015-1276	Use-after-free vulnerability in content/browser/indexed_db/indexed_db_backing_store.cc in the IndexedDB implementation in Google Chrome before 44.0.2403.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging an abort action before a certain write operation.
CVE-2015-1277	Use-after-free vulnerability in the accessibility implementation in Google Chrome before 44.0.2403.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging lack of certain validity checks for accessibility-tree data structures.
CVE-2015-1278	content/browser/web_contents/web_contents_impl.cc in Google Chrome before 44.0.2403.89 does not ensure that a PDF document's modal dialog is closed upon navigation to an interstitial page, which allows remote attackers to spoof URLs via a crafted document, as demonstrated by the alert_dialog.pdf document.
CVE-2015-1279	Integer overflow in the CJBig2_Image::expand function in fxcodec/jbig2/JBig2_Image.cpp in PDFium, as used in Google Chrome before 44.0.2403.89, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via large height and stride values.
CVE-2015-1280	SkPictureShader.cpp in Skia, as used in Google Chrome before 44.0.2403.89, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging access to a renderer process and providing crafted serialized data.
CVE-2015-1281	core/loader/ImageLoader.cpp in Blink, as used in Google Chrome before 44.0.2403.89, does not properly determine the V8 context of a microtask, which allows remote attackers to bypass Content Security Policy (CSP) restrictions by providing an image from an unintended source.

CVE-2015-1282	Multiple use-after-free vulnerabilities in fpdfsdk/src/javascript/Document.cpp in PDFium, as used in Google Chrome before 44.0.2403.89, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document, related to the (1) Document::delay and (2) Document::DoFieldDelay functions.
CVE-2015-1283	Multiple integer overflows in the XML_GetBuffer function in Expat through 2.1.0, as used in Google Chrome before 44.0.2403.89 and other products, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted XML data, a related issue to CVE-2015-2716.
CVE-2015-1284	The LocalFrame::isURLAllowed function in core/frame/LocalFrame.cpp in Blink, as used in Google Chrome before 44.0.2403.89, does not properly check for a page's maximum number of frames, which allows remote attackers to cause a denial of service (invalid count value and use-after-free) or possibly have unspecified other impact via crafted JavaScript code that makes many createElement calls for IFRAME elements.
CVE-2015-1285	The XSSAuditor::canonicalize function in core/html/parser/XSSAuditor.cpp in the XSS auditor in Blink, as used in Google Chrome before 44.0.2403.89, does not properly choose a truncation point, which makes it easier for remote attackers to obtain sensitive information via an unspecified linear-time attack.
CVE-2015-1286	Cross-site scripting (XSS) vulnerability in the V8ContextNativeHandler::GetModuleSystem function in extensions/renderer/v8_context_native_handler.cc in Google Chrome before 44.0.2403.89 allows remote attackers to inject arbitrary web script or HTML by leveraging the lack of a certain V8 context restriction, aka a Blink "Universal XSS (UXSS)."
CVE-2015-1287	Blink, as used in Google Chrome before 44.0.2403.89, enables a quirks-mode exception that limits the cases in which a Cascading Style Sheets (CSS) document is required to have the text/css content type, which allows remote attackers to bypass the Same Origin Policy via a crafted web site, related to core/fetch/CSSStyleSheetResource.cpp.
CVE-2015-1288	The Spellcheck API implementation in Google Chrome before 44.0.2403.89 does not use an HTTPS session for downloading a Hunspell dictionary, which allows man-in-the-middle attackers to deliver incorrect spelling suggestions or possibly have unspecified other impact via a crafted file, a related issue to CVE-2015-1263.

CVE-2015-1289	Multiple unspecified vulnerabilities in Google Chrome before 44.0.2403.89 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1290	The Google V8 engine, as used in Google Chrome before 44.0.2403.89 and QtWebEngineCore in Qt before 5.5.1, allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via a crafted web site.
CVE-2015-1291	The ContainerNode::parserRemoveChild function in core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 45.0.2454.85, does not check whether a node is expected, which allows remote attackers to bypass the Same Origin Policy or cause a denial of service (DOM tree corruption) via a web site with crafted JavaScript code and IFRAME elements.
CVE-2015-1292	The NavigatorServiceWorker::serviceWorker function in modules/serviceworkers/NavigatorServiceWorker.cpp in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to bypass the Same Origin Policy by accessing a Service Worker.
CVE-2015-1293	The DOM implementation in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2015-1294	Use-after-free vulnerability in the SkMatrix::invertNonIdentity function in core/SkMatrix.cpp in Skia, as used in Google Chrome before 45.0.2454.85, allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering the use of matrix elements that lead to an infinite result during an inversion calculation.
CVE-2015-1295	Multiple use-after-free vulnerabilities in the PrintWebViewHelper class in components/printing/renderer/print_web_view_helper.cc in Google Chrome before 45.0.2454.85 allow user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact by triggering nested IPC messages during preparation for printing, as demonstrated by messages associated with PDF documents in conjunction with messages about printer capabilities.
CVE-2015-1296	The UnescapeURLWithAdjustmentsImpl implementation in net/base/escape.cc in Google Chrome before 45.0.2454.85 does not prevent display of Unicode LOCK characters in the omnibox, which makes it easier for remote attackers to spoof the SSL lock icon by placing one of these characters at the end of a URL, as demonstrated by the omnibox in localizations for right-to-left languages.

CVE-2015-1297	The WebRequest API implementation in extensions/browser/api/web_request/web_request_api.cc in Google Chrome before 45.0.2454.85 does not properly consider a request's source before accepting the request, which allows remote attackers to bypass intended access restrictions via a crafted (1) app or (2) extension.
CVE-2015-1298	The RuntimeEventRouter::OnExtensionUninstalled function in extensions/browser/api/runtime/runtime_api.cc in Google Chrome before 45.0.2454.85 does not ensure that the setUninstallURL preference corresponds to the URL of a web site, which allows user-assisted remote attackers to trigger access to an arbitrary URL via a crafted extension that is uninstalled.
CVE-2015-1299	Use-after-free vulnerability in the shared-timer implementation in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging erroneous timer firing, related to ThreadTimers.cpp and Timer.cpp.
CVE-2015-1300	The FrameFetchContext::updateTimingInfoForIFrameNavigation function in core/loader/FrameFetchContext.cpp in Blink, as used in Google Chrome before 45.0.2454.85, does not properly restrict the availability of IFRAME Resource Timing API times, which allows remote attackers to obtain sensitive information via crafted JavaScript code that leverages a history.back call.
CVE-2015-1301	Multiple unspecified vulnerabilities in Google Chrome before 45.0.2454.85 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1302	The PDF viewer in Google Chrome before 46.0.2490.86 does not properly restrict scripting messages and API exposure, which allows remote attackers to bypass the Same Origin Policy via an unintended embedder or unintended plugin loading, related to pdf.js and out_of_process_instance.cc.
CVE-2015-1303	bindings/core/v8/V8DOMWrapper.h in Blink, as used in Google Chrome before 45.0.2454.101, does not perform a rethrow action to propagate information about a cross-context exception, which allows remote attackers to bypass the Same Origin Policy via a crafted HTML document containing an IFRAME element.
CVE-2015-1304	object-observe.js in Google V8, as used in Google Chrome before 45.0.2454.101, does not properly restrict method calls on access-checked objects, which allows remote attackers to bypass the Same Origin Policy via a (1) observe or (2) getNotifier call.

CVE-2015-1346	Multiple unspecified vulnerabilities in Google V8 before 3.30.33.15, as used in Google Chrome before 40.0.2214.91, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1359	Multiple off-by-one errors in fpdfapi/fpdf_font/font_int.h in PDFium, as used in Google Chrome before 40.0.2214.91, allow remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a crafted PDF document, related to an "intra-object-overflow" issue, a different vulnerability than CVE-2015-1205.
CVE-2015-1360	Skia, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via crafted data that is improperly handled during text drawing, related to gpu/GrBitmapTextContext.cpp and gpu/GrDistanceFieldTextContext.cpp, a different vulnerability than CVE-2015-1205.
CVE-2015-1361	platform/image-decoders/ImageFrame.h in Blink, as used in Google Chrome before 40.0.2214.91, does not initialize a variable that is used in calls to the Skia SkBitmap::setAlphaType function, which might allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted HTML document, a different vulnerability than CVE-2015-1205.
CVE-2015-1427	The Groovy scripting engine in Elasticsearch before 1.3.8 and 1.4.x before 1.4.3 allows remote attackers to bypass the sandbox protection mechanism and execute arbitrary shell commands via a crafted script.
CVE-2015-2238	Multiple unspecified vulnerabilities in Google V8 before 4.1.0.21, as used in Google Chrome before 41.0.2272.76, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-2239	Google Chrome before 41.0.2272.76, when Instant Extended mode is used, does not properly consider the interaction between the "1993 search" features and restore-from-disk RELOAD transitions, which makes it easier for remote attackers to spoof the address bar for a search-results page by leveraging (1) a compromised search engine or (2) an XSS vulnerability in a search engine, a different vulnerability than CVE-2015-1231.
CVE-2015-3038	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different

	vulnerability than CVE-2015-0347, CVE-2015-0350, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3041, CVE-2015-3042, and CVE-2015-3043.
CVE-2015-3039	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0349, CVE-2015-0351, and CVE-2015-0358.
CVE-2015-3040	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux does not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors, a different vulnerability than CVE-2015-0357.
CVE-2015-3041	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0347, CVE-2015-0350, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3042, and CVE-2015-3043.
CVE-2015-3042	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0347, CVE-2015-0350, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, and CVE-2015-3043.
CVE-2015-3043	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as exploited in the wild in April 2015, a different vulnerability than CVE-2015-0347, CVE-2015-0350, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, and CVE-2015-3042.
CVE-2015-3044	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors.

CVE-2015-3077	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3084 and CVE-2015-3086.
CVE-2015-3078	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3089, CVE-2015-3090, and CVE-2015-3093.
CVE-2015-3079	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors.
CVE-2015-3080	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-3081	Race condition in Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allows attackers to bypass the Internet Explorer Protected Mode protection mechanism via unspecified vectors.
CVE-2015-3082	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow remote attackers to bypass intended restrictions on filesystem write operations via unspecified vectors, a different vulnerability than CVE-2015-3083 and CVE-2015-3085.
CVE-2015-3083	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before

	17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow remote attackers to bypass intended restrictions on filesystem write operations via unspecified vectors, a different vulnerability than CVE-2015-3082 and CVE-2015-3085.
CVE-2015-3084	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3077 and CVE-2015-3086.
CVE-2015-3085	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow remote attackers to bypass intended restrictions on filesystem write operations via unspecified vectors, a different vulnerability than CVE-2015-3082 and CVE-2015-3083.
CVE-2015-3086	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3077 and CVE-2015-3084.
CVE-2015-3087	Integer overflow in Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-3088	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-3089	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow attackers to execute arbitrary code or cause a

	denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3078, CVE-2015-3090, and CVE-2015-3093.
CVE-2015-3090	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3078, CVE-2015-3089, and CVE-2015-3093.
CVE-2015-3091	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors, a different vulnerability than CVE-2015-3092.
CVE-2015-3092	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors, a different vulnerability than CVE-2015-3091.
CVE-2015-3093	Adobe Flash Player before 13.0.0.289 and 14.x through 17.x before 17.0.0.188 on Windows and OS X and before 11.2.202.460 on Linux, Adobe AIR before 17.0.0.172, Adobe AIR SDK before 17.0.0.172, and Adobe AIR SDK & Compiler before 17.0.0.172 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3078, CVE-2015-3089, and CVE-2015-3090.
CVE-2015-3096	Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allow remote attackers to bypass a CVE-2014-5333 protection mechanism via unspecified vectors.
CVE-2015-3098	Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and

	before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allow remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-3099 and CVE-2015-3102.
CVE-2015-3099	Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allow remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-3098 and CVE-2015-3102.
CVE-2015-3100	Stack-based buffer overflow in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-3101	The Flash broker in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, when Internet Explorer is used, allows attackers to perform a transition from Low Integrity to Medium Integrity via unspecified vectors.
CVE-2015-3102	Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allow remote attackers to bypass the Same Origin Policy via unspecified

	vectors, a different vulnerability than CVE-2015-3098 and CVE-2015-3099.
CVE-2015-3103	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3106 and CVE-2015-3107.
CVE-2015-3104	Integer overflow in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-3105	Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2015-3106	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3103 and CVE-2015-3107.
CVE-2015-3107	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK &

	Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3103 and CVE-2015-3106.
CVE-2015-3108	Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors.
CVE-2015-3113	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.296 and 14.x through 18.x before 18.0.0.194 on Windows and OS X and before 11.2.202.468 on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in June 2015.
CVE-2015-3114	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors.
CVE-2015-3115	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2014-0578, CVE-2015-3116, CVE-2015-3125, and CVE-2015-5116.
CVE-2015-3116	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2014-0578, CVE-2015-3115, CVE-2015-3125, and CVE-2015-5116.
CVE-2015-3117	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180

	allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, CVE-2015-3134, and CVE-2015-4431.
CVE-2015-3118	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.
CVE-2015-3119	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3120, CVE-2015-3121, CVE-2015-3122, and CVE-2015-4433.
CVE-2015-3120	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3119, CVE-2015-3121, CVE-2015-3122, and CVE-2015-4433.
CVE-2015-3121	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3119, CVE-2015-3120, CVE-2015-3122, and CVE-2015-4433.
CVE-2015-3122	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different

	vulnerability than CVE-2015-3119, CVE-2015-3120, CVE-2015-3121, and CVE-2015-4433.
CVE-2015-3123	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3130, CVE-2015-3133, CVE-2015-3134, and CVE-2015-4431.
CVE-2015-3124	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.
CVE-2015-3125	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2014-0578, CVE-2015-3115, CVE-2015-3116, and CVE-2015-5116.
CVE-2015-3126	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2015-4429.
CVE-2015-3127	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3128, CVE-2015-3129,

	CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.
CVE-2015-3128	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.
CVE-2015-3129	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.
CVE-2015-3130	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3133, CVE-2015-3134, and CVE-2015-4431.
CVE-2015-3131	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.
CVE-2015-3132	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before

	18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.
CVE-2015-3133	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3134, and CVE-2015-4431.
CVE-2015-3134	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, and CVE-2015-4431.
CVE-2015-3135	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-4432 and CVE-2015-5118.
CVE-2015-3136	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3137, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.

CVE-2015-3137	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-4428, CVE-2015-4430, and CVE-2015-5117.
CVE-2015-3333	Multiple unspecified vulnerabilities in Google V8 before 4.2.77.14, as used in Google Chrome before 42.0.2311.90, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-3334	browser/ui/website_settings/website_settings.cc in Google Chrome before 42.0.2311.90 does not always display "Media: Allowed by you" in a Permissions table after the user has granted camera permission to a web site, which might make it easier for user-assisted remote attackers to obtain sensitive video data from a device's physical environment via a crafted web site that turns on the camera at a time when the user believes that camera access is prohibited.
CVE-2015-3335	The NaClSandbox::InitializeLayerTwoSandbox function in components/nacl/loader/sandbox_linux/nacl_sandbox_linux.cc in Google Chrome before 42.0.2311.90 does not have RLIMIT_AS and RLIMIT_DATA limits for Native Client (aka NaCl) processes, which might make it easier for remote attackers to conduct row-hammer attacks or have unspecified other impact by leveraging the ability to run a crafted program in the NaCl sandbox.
CVE-2015-3336	Google Chrome before 42.0.2311.90 does not always ask the user before proceeding with CONTENT_SETTINGS_TYPE_FULLSCREEN and CONTENT_SETTINGS_TYPE_MOUSELOCK changes, which allows user-assisted remote attackers to cause a denial of service (UI disruption) by constructing a crafted HTML document containing JavaScript code with requestFullScreen and requestPointerLock calls, and arranging for the user to access this document with a file: URL.
CVE-2015-3337	Directory traversal vulnerability in Elasticsearch before 1.4.5 and 1.5.x before 1.5.2, when a site plugin is enabled, allows remote attackers to read arbitrary files via unspecified vectors.
CVE-2015-3910	Multiple unspecified vulnerabilities in Google V8 before 4.3.61.21, as used in Google Chrome before

	43.0.2357.65, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-4165	The snapshot API in Elasticsearch before 1.6.0 when another application exists on the system that can read Lucene files and execute code from them, is accessible by the attacker, and the Java VM on which Elasticsearch is running can write to a location that the other application can read and execute from, allows remote authenticated users to write to and create arbitrary snapshot metadata files, and potentially execute arbitrary code.
CVE-2015-4428	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4430, and CVE-2015-5117.
CVE-2015-4429	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2015-3126.
CVE-2015-4430	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, and CVE-2015-5117.
CVE-2015-4431	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a

	denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, and CVE-2015-3134.
CVE-2015-4432	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3135 and CVE-2015-5118.
CVE-2015-4433	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3119, CVE-2015-3120, CVE-2015-3121, and CVE-2015-3122.
CVE-2015-4852	The WLS Security component in Oracle WebLogic Server 10.3.6.0, 12.1.2.0, 12.1.3.0, and 12.2.1.0 allows remote attackers to execute arbitrary commands via a crafted serialized Java object in T3 protocol traffic to TCP port 7001, related to oracle_common/modules/com.bea.core.apache.commons.collections.jar. NOTE: the scope of this CVE is limited to the WebLogic Server product.
CVE-2015-5116	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2014-0578, CVE-2015-3115, CVE-2015-3116, and CVE-2015-3125.
CVE-2015-5117	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, and CVE-2015-4430.

CVE-2015-5118	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3135 and CVE-2015-4432.
CVE-2015-5119	Use-after-free vulnerability in the ByteArray class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.296 and 14.x through 18.0.0.194 on Windows and OS X and 11.x through 11.2.202.468 on Linux allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content that overrides a valueOf function, as exploited in the wild in July 2015.
CVE-2015-5122	Use-after-free vulnerability in the DisplayObject class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.302 on Windows and OS X, 14.x through 18.0.0.203 on Windows and OS X, 11.x through 11.2.202.481 on Linux, and 12.x through 18.0.0.204 on Linux Chrome installations allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content that leverages improper handling of the opaqueBackground property, as exploited in the wild in July 2015.
CVE-2015-5123	Use-after-free vulnerability in the BitmapData class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.302 on Windows and OS X, 14.x through 18.0.0.203 on Windows and OS X, 11.x through 11.2.202.481 on Linux, and 12.x through 18.0.0.204 on Linux Chrome installations allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content that overrides a valueOf function, as exploited in the wild in July 2015.
CVE-2015-5124	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, CVE-2015-3134, and CVE-2015-4431.
CVE-2015-5125	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR

	before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to cause a denial of service (vector-length corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2015-5127	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5129	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5541.
CVE-2015-5130	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5131	Buffer overflow in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5132 and CVE-2015-5133.
CVE-2015-5132	Buffer overflow in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors,

	a different vulnerability than CVE-2015-5131 and CVE-2015-5133.
CVE-2015-5133	Buffer overflow in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5131 and CVE-2015-5132.
CVE-2015-5134	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5377	** DISPUTED ** Elasticsearch before 1.6.1 allows remote attackers to execute arbitrary code via unspecified vectors involving the transport protocol. NOTE: ZDI appears to claim that CVE-2015-3253 and CVE-2015-5377 are the same vulnerability.
CVE-2015-5531	Directory traversal vulnerability in Elasticsearch before 1.6.1 allows remote attackers to read arbitrary files via unspecified vectors related to snapshot API calls.
CVE-2015-5539	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5540	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5550, CVE-2015-5551,

	CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5541	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5129.
CVE-2015-5544	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5552, and CVE-2015-5553.
CVE-2015-5545	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5544, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5552, and CVE-2015-5553.
CVE-2015-5546	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5544, CVE-2015-5545, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5552, and CVE-2015-5553.
CVE-2015-5547	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5548, CVE-2015-5549, CVE-2015-5552, and CVE-2015-5553.

CVE-2015-5548	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5549, CVE-2015-5552, and CVE-2015-5553.
CVE-2015-5549	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5552, and CVE-2015-5553.
CVE-2015-5550	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5551	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5552	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than

	CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, and CVE-2015-5553.
CVE-2015-5553	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5544, CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, and CVE-2015-5552.
CVE-2015-5554	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-5555, CVE-2015-5558, and CVE-2015-5562.
CVE-2015-5555	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-5554, CVE-2015-5558, and CVE-2015-5562.
CVE-2015-5556	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5557	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5559,

	CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5558	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-5554, CVE-2015-5555, and CVE-2015-5562.
CVE-2015-5559	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5560	Integer overflow in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-5561	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5562	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-5554, CVE-2015-5555, and CVE-2015-5558.
CVE-2015-5563	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before

	18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5564	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, and CVE-2015-5565.
CVE-2015-5565	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, and CVE-2015-5564.
CVE-2015-5566	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5567	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service

	(stack memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5579.
CVE-2015-5568	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to cause a denial of service (vector-length corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2015-5569	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 improperly implement the Flash broker API, which has unspecified impact and attack vectors.
CVE-2015-5570	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5574, CVE-2015-5581, CVE-2015-5584, and CVE-2015-6682.
CVE-2015-5571	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 do not properly restrict the SWF file format, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks against JSONP endpoints, and obtain sensitive information, via a crafted OBJECT element with SWF content satisfying the character-set requirements of a callback API. NOTE: this issue exists because of an incomplete fix for CVE-2014-4671 and CVE-2014-5333.
CVE-2015-5572	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors.
CVE-2015-5573	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to

	execute arbitrary code by leveraging an unspecified "type confusion."
CVE-2015-5574	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5581, CVE-2015-5584, and CVE-2015-6682.
CVE-2015-5575	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.
CVE-2015-5576	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors.
CVE-2015-5577	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.
CVE-2015-5578	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5580, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.
CVE-2015-5579	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before

	11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5567.
CVE-2015-5580	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.
CVE-2015-5581	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5574, CVE-2015-5584, and CVE-2015-6682.
CVE-2015-5582	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5588, and CVE-2015-6677.
CVE-2015-5584	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5574, CVE-2015-5581, and CVE-2015-6682.
CVE-2015-5587	Stack-based buffer overflow in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors.

CVE-2015-5588	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, and CVE-2015-6677.
CVE-2015-5605	The regular-expression implementation in Google V8, as used in Google Chrome before 44.0.2403.89, mishandles interrupts, which allows remote attackers to cause a denial of service (application crash) via crafted JavaScript code, as demonstrated by an error in garbage collection during allocation of a stack-overflow exception message.
CVE-2015-6580	Multiple unspecified vulnerabilities in Google V8 before 4.5.103.29, as used in Google Chrome before 45.0.2454.85, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-6581	Double free vulnerability in the opj_j2k_copy_default_tcp_and_create_tcd function in j2k.c in OpenJPEG before r3002, as used in PDFium in Google Chrome before 45.0.2454.85, allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by triggering a memory-allocation failure.
CVE-2015-6582	The decompose function in platform/transforms/TransformationMatrix.cpp in Blink, as used in Google Chrome before 45.0.2454.85, does not verify that a matrix inversion succeeded, which allows remote attackers to cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified other impact via a crafted web site.
CVE-2015-6583	Google Chrome before 45.0.2454.85 does not display a location bar for a hosted app's window after navigation away from the installation site, which might make it easier for remote attackers to spoof content via a crafted app, related to browser.cc and hosted_app_browser_controller.cc.
CVE-2015-6676	Buffer overflow in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-6678.

CVE-2015-6677	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, and CVE-2015-5588.
CVE-2015-6678	Buffer overflow in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-6676.
CVE-2015-6679	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to bypass the Same Origin Policy and obtain sensitive information via unspecified vectors.
CVE-2015-6682	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5574, CVE-2015-5581, and CVE-2015-5584.
CVE-2015-6755	The ContainerNode::parserInsertBefore function in core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 46.0.2490.71, proceeds with a DOM tree insertion in certain cases where a parent node no longer contains a child node, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.
CVE-2015-6756	Use-after-free vulnerability in the CPDFSDK_PageView implementation in fpdfsdk/src/fsdk_mgr.cpp in PDFium, as used in Google Chrome before 46.0.2490.71, allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by leveraging mishandling of a focused annotation in a PDF document.
CVE-2015-6757	Use-after-free vulnerability in content/browser/service_worker/embedded_worker_instance.cc in the ServiceWorker implementation in Google Chrome

	before 46.0.2490.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging object destruction in a callback.
CVE-2015-6758	The CPDF_Document::GetPage function in fpdfapi/ fpdf_parser/fpdf_parser_document.cpp in PDFium, as used in Google Chrome before 46.0.2490.71, does not properly perform a cast of a dictionary object, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.
CVE-2015-6759	The shouldTreatAsUniqueOrigin function in platform/ weborigin/SecurityOrigin.cpp in Blink, as used in Google Chrome before 46.0.2490.71, does not ensure that the origin of a LocalStorage resource is considered unique, which allows remote attackers to obtain sensitive information via vectors involving a blob: URL.
CVE-2015-6760	The Image11::map function in renderer/d3d/d3d11/ Image11.cpp in libANGLE, as used in Google Chrome before 46.0.2490.71, mishandles mapping failures after device-lost events, which allows remote attackers to cause a denial of service (invalid read or write) or possibly have unspecified other impact via vectors involving a removed device.
CVE-2015-6761	The update_dimensions function in libavcodec/ vp8.c in FFmpeg through 2.8.1, as used in Google Chrome before 46.0.2490.71 and other products, relies on a coefficient-partition count during multi-threaded operation, which allows remote attackers to cause a denial of service (race condition and memory corruption) or possibly have unspecified other impact via a crafted WebM file.
CVE-2015-6762	The CSSFontFaceSrcValue::fetch function in core/css/ CSSFontFaceSrcValue.cpp in the Cascading Style Sheets (CSS) implementation in Blink, as used in Google Chrome before 46.0.2490.71, does not use the CORS cross-origin request algorithm when a font's URL appears to be a same-origin URL, which allows remote web servers to bypass the Same Origin Policy via a redirect.
CVE-2015-6763	Multiple unspecified vulnerabilities in Google Chrome before 46.0.2490.71 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-6764	The BasicJsonStringifier::SerializeJSArray function in json-stringifier.h in the JSON stringifier in Google V8, as used in Google Chrome before 47.0.2526.73, improperly loads array elements, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted JavaScript code.

CVE-2015-6765	Use-after-free vulnerability in content/browser/appcache/appcache_update_job.cc in Google Chrome before 47.0.2526.73 allows remote attackers to execute arbitrary code or cause a denial of service by leveraging the mishandling of AppCache update jobs.
CVE-2015-6766	Use-after-free vulnerability in the AppCache implementation in Google Chrome before 47.0.2526.73 allows remote attackers with renderer access to cause a denial of service or possibly have unspecified other impact by leveraging incorrect AppCacheUpdateJob behavior associated with duplicate cache selection.
CVE-2015-6767	Use-after-free vulnerability in content/browser/appcache/appcache_dispatcher_host.cc in the AppCache implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect pointer maintenance associated with certain callbacks.
CVE-2015-6768	The DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-6770.
CVE-2015-6769	The provisional-load commit implementation in WebKit/Source/bindings/core/v8/WindowProxy.cpp in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy by leveraging a delay in window proxy clearing.
CVE-2015-6770	The DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-6768.
CVE-2015-6771	js/array.js in Google V8, as used in Google Chrome before 47.0.2526.73, improperly implements certain map and filter operations for arrays, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2015-6772	The DOM implementation in Blink, as used in Google Chrome before 47.0.2526.73, does not prevent javascript: URL navigation while a document is being detached, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code that improperly interacts with a plugin.
CVE-2015-6773	The convolution implementation in Skia, as used in Google Chrome before 47.0.2526.73, does not properly constrain row lengths, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted graphics data.

CVE-2015-6774	Use-after-free vulnerability in the GetLoadTimes function in renderer/loadtimes_extension_bindings.cc in the Extensions implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that modifies a pointer used for reporting loadTimes data.
CVE-2015-6775	fpdfsdk/src/jsapi/fxjs_v8.cpp in PDFium, as used in Google Chrome before 47.0.2526.73, does not use signatures, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2015-6776	The opj_dwt_decode_1* functions in dwt.c in OpenJPEG, as used in PDFium in Google Chrome before 47.0.2526.73, allow remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG 2000 data that is mishandled during a discrete wavelet transform.
CVE-2015-6777	Use-after-free vulnerability in the ContainerNode::notifyNodeInsertedInternal function in WebKit/Source/core/dom/ContainerNode.cpp in the DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOMCharacterDataModified events for certain detached-subtree insertions.
CVE-2015-6778	The CJBig2_SymbolDict class in fxcodec/jbig2/JBig2_SymbolDict.cpp in PDFium, as used in Google Chrome before 47.0.2526.73, allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via a PDF document containing crafted data with JBIG2 compression.
CVE-2015-6779	PDFium, as used in Google Chrome before 47.0.2526.73, does not properly restrict use of chrome: URLs, which allows remote attackers to bypass intended scheme restrictions via a crafted PDF document, as demonstrated by a document with a link to a chrome://settings URL.
CVE-2015-6780	Use-after-free vulnerability in the Infobars implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site, related to browser/ui/views/website_settings/website_settings_popup_view.cc.
CVE-2015-6781	Integer overflow in the FontData::Bound function in data/font_data.cc in Google sfntly, as used in Google Chrome before 47.0.2526.73, allows remote attackers to cause a denial of service or possibly have

	unspecified other impact via a crafted offset or length value within font data in an SFNT container.
CVE-2015-6782	The Document::open function in WebKit/Source/core/dom/Document.cpp in Google Chrome before 47.0.2526.73 does not ensure that page-dismissal event handling is compatible with modal-dialog blocking, which makes it easier for remote attackers to spoof Omnibox content via a crafted web site.
CVE-2015-6784	The page serializer in Google Chrome before 47.0.2526.73 mishandles Mark of the Web (MOTW) comments for URLs containing a "--" sequence, which might allow remote attackers to inject HTML via a crafted URL, as demonstrated by an initial http://example.com?-- substring.
CVE-2015-6785	The CSPSource::hostMatches function in WebKit/Source/core/frame/csp/CSPSource.cpp in the Content Security Policy (CSP) implementation in Google Chrome before 47.0.2526.73 accepts an x.y hostname as a match for a *.x.y pattern, which might allow remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging a policy that was intended to be specific to subdomains.
CVE-2015-6786	The CSPSourceList::matches function in WebKit/Source/core/frame/csp/CSPSourceList.cpp in the Content Security Policy (CSP) implementation in Google Chrome before 47.0.2526.73 accepts a blob:, data:, or filesystem: URL as a match for a * pattern, which allows remote attackers to bypass intended scheme restrictions in opportunistic circumstances by leveraging a policy that relies on this pattern.
CVE-2015-6787	Multiple unspecified vulnerabilities in Google Chrome before 47.0.2526.73 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-6788	The ObjectBackedNativeHandler class in extensions/renderer/object_backed_native_handler.cc in the extensions subsystem in Google Chrome before 47.0.2526.80 improperly implements handler functions, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2015-6789	Race condition in the MutationObserver implementation in Blink, as used in Google Chrome before 47.0.2526.80, allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact by leveraging unanticipated object deletion.
CVE-2015-6790	The WebPageSerializerImpl::openTagToString function in WebKit/Source/web/WebPageSerializerImpl.cpp in the page serializer in Google Chrome before

	47.0.2526.80 does not properly use HTML entities, which might allow remote attackers to inject arbitrary web script or HTML via a crafted document, as demonstrated by a double-quote character inside a single-quoted string.
CVE-2015-6791	Multiple unspecified vulnerabilities in Google Chrome before 47.0.2526.80 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-6792	The MIDI subsystem in Google Chrome before 47.0.2526.106 does not properly handle the sending of data, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors, related to midi_manager.cc, midi_manager_alsa.cc, and midi_manager_mac.cc, a different vulnerability than CVE-2015-8664.
CVE-2015-7625	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7626, CVE-2015-7627, CVE-2015-7630, CVE-2015-7633, and CVE-2015-7634.
CVE-2015-7626	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7627, CVE-2015-7630, CVE-2015-7633, and CVE-2015-7634.
CVE-2015-7627	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7626, CVE-2015-7630, CVE-2015-7633, and CVE-2015-7634.
CVE-2015-7628	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow remote

	attackers to bypass the Same Origin Policy and obtain sensitive information via unspecified vectors.
CVE-2015-7629	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via a TextFormat object with a crafted tabStops property, a different vulnerability than CVE-2015-7631, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7630	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7633, and CVE-2015-7634.
CVE-2015-7631	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via a TextLine object with a crafted validity property, a different vulnerability than CVE-2015-7629, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7632	Buffer overflow in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via a Loader object with a crafted loaderBytes property.
CVE-2015-7633	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7630, and CVE-2015-7634.
CVE-2015-7634	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213,

	and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7630, and CVE-2015-7633.
CVE-2015-7635	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7636	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7637	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7638	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.

CVE-2015-7639	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7640	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7641	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7642	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7643	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via a Video object with a crafted deblocking

	property, a different vulnerability than CVE-2015-7629, CVE-2015-7631, and CVE-2015-7644.
CVE-2015-7644	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, and CVE-2015-7643.
CVE-2015-7645	Adobe Flash Player 18.x through 18.0.0.252 and 19.x through 19.0.0.207 on Windows and OS X and 11.x through 11.2.202.535 on Linux allows remote attackers to execute arbitrary code via a crafted SWF file, as exploited in the wild in October 2015.
CVE-2015-7647	Adobe Flash Player before 18.0.0.255 and 19.x before 19.0.0.226 on Windows and OS X and before 11.2.202.540 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-7648.
CVE-2015-7648	Adobe Flash Player before 18.0.0.255 and 19.x before 19.0.0.226 on Windows and OS X and before 11.2.202.540 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-7647.
CVE-2015-7651	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted DefineFunction atoms, a different vulnerability than CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7652	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via a crafted gridFitType property value, a different vulnerability than CVE-2015-7651, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658,

	CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7653	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted globalToLocal arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7654	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted attachSound arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7655	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted actionExtends arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7656	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted actionImplementsOp arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7657, CVE-2015-7658,

	CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7657	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted actionCallMethod arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7658	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted actionInstanceOf arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7659	Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion" in the NetConnection object implementation.
CVE-2015-7660	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted setMask arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.

CVE-2015-7661	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via a crafted getBounds call, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7662	Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allow remote attackers to bypass intended access restrictions and write to files via unspecified vectors.
CVE-2015-7663	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7834	Multiple unspecified vulnerabilities in Google V8 before 4.6.85.23, as used in Google Chrome before 46.0.2490.71, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-8011	Buffer overflow in the lldp_decode function in daemon/protocols/lldp.c in lldpd before 0.8.0 allows remote attackers to cause a denial of service (daemon crash) and possibly execute arbitrary code via vectors involving large management addresses and TLV boundaries.
CVE-2015-8042	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via a crafted loadSound call, a different vulnerability than CVE-2015-7651,

	CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-8043	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-8044	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, and CVE-2015-8046.
CVE-2015-8045	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8046	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660,

	CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, and CVE-2015-8044.
CVE-2015-8047	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8048	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8049	Use-after-free vulnerability in the TextField object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted autoSize property value, a different vulnerability than CVE-2015-8048, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064,

	CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8050	Use-after-free vulnerability in the MovieClip object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted beginGradientFill call, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8055	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061,

	CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8056	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8057	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061,

	CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8058	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8059	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8061,

	CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8060	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8061	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447,

	CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8062	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8063	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447,

	CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8064	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8065	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447,

	CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8066	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8067	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447,

	CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8068	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8069	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447,

	CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8070	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8071	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447,

	CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8126	Multiple buffer overflows in the (1) png_set_PLTE and (2) png_get_PLTE functions in libpng before 1.0.64, 1.1.x and 1.2.x before 1.2.54, 1.3.x and 1.4.x before 1.4.17, 1.5.x before 1.5.24, and 1.6.x before 1.6.19 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a small bit-depth value in an IHDR (aka image header) chunk in a PNG image.
CVE-2015-8401	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8402	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411,

	CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8403	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8404	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411,

	CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8405	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8406	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8410, CVE-2015-8411,

	CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8407	Stack-based buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8457.
CVE-2015-8408	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8409	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2015-8440 and CVE-2015-8453.
CVE-2015-8410	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401,

	CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8411	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8412	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401,

	CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8413	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8414	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401,

	CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8415	Buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-8416	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8417	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8418	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408,

	CVE-2015-8416, CVE-2015-8417, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8419	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8420	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8421	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063,

	CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8422	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8423	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063,

	CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8424	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8425	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063,

	CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8426	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8427	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063,

	CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8428	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8429	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063,

	CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8430	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8431	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063,

	CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8432	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8433	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063,

	CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8434	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8435	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063,

	CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8436	Use-after-free vulnerability in the PrintJob object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted addPage arguments, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8437	Use-after-free vulnerability in the Selection object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted setFocus call, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057,

	CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8438	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted XML object that is mishandled during a toString call, a different vulnerability than CVE-2015-8446.
CVE-2015-8439	The SharedObject object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code by leveraging an unspecified "type confusion" during a getRemote call, a different vulnerability than CVE-2015-8456.
CVE-2015-8440	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2015-8409 and CVE-2015-8453.
CVE-2015-8441	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056,

	CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8442	Use-after-free vulnerability in the MovieClip object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted filters property value, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8443	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045,

	CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8444	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8445	Integer overflow in the Shader filter implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a large BitmapData source object.
CVE-2015-8446	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via an MP3 file with COMM tags that are mishandled during memory allocation, a different vulnerability than CVE-2015-8438.
CVE-2015-8447	Use-after-free vulnerability in the Color object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted setTransform arguments, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421,

	CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8448	Use-after-free vulnerability in the DisplacementMapFilter object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted mapBitmap property value, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8449	Use-after-free vulnerability in the MovieClip object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted lineTo method call, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404,

	CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8450	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted filters property value in a TextField object, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8451	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, and CVE-2015-8455.
CVE-2015-8452	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228

	on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, and CVE-2015-8454.
CVE-2015-8453	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to bypass the ASLR protection mechanism via JIT data, a different vulnerability than CVE-2015-8409 and CVE-2015-8440.
CVE-2015-8454	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427,

	CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, and CVE-2015-8452.
CVE-2015-8455	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, and CVE-2015-8451.
CVE-2015-8456	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-8439.
CVE-2015-8457	Stack-based buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8407.
CVE-2015-8459	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8460, CVE-2015-8636, and CVE-2015-8645.
CVE-2015-8460	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified

	vectors, a different vulnerability than CVE-2015-8459, CVE-2015-8636, and CVE-2015-8645.
CVE-2015-8478	Multiple unspecified vulnerabilities in Google V8 before 4.7.80.23, as used in Google Chrome before 47.0.2526.73, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-8479	Use-after-free vulnerability in the AudioOutputDevice::OnDeviceAuthorized function in media/audio/audio_output_device.cc in Google Chrome before 47.0.2526.73 allows attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by triggering access to an unauthorized audio output device.
CVE-2015-8480	The VideoFramePool::PoolImpl::CreateFrame function in media/base/video_frame_pool.cc in Google Chrome before 47.0.2526.73 does not initialize memory for a video-frame data structure, which might allow remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact by leveraging improper interaction with the vp3_h_loop_filter_c function in libavcodec/vp3dsp.c in FFmpeg.
CVE-2015-8548	Multiple unspecified vulnerabilities in Google V8 before 4.7.80.23, as used in Google Chrome before 47.0.2526.80, allow attackers to cause a denial of service or possibly have other impact via unknown vectors, a different issue than CVE-2015-8478.
CVE-2015-8634	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.
CVE-2015-8635	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646,

	CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.
CVE-2015-8636	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8459, CVE-2015-8460, and CVE-2015-8645.
CVE-2015-8638	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.
CVE-2015-8639	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.
CVE-2015-8640	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.
CVE-2015-8641	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR

	SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.
CVE-2015-8642	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.
CVE-2015-8643	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.
CVE-2015-8644	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion."
CVE-2015-8645	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8459, CVE-2015-8460, and CVE-2015-8636.
CVE-2015-8646	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on

	Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.
CVE-2015-8647	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.
CVE-2015-8648	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8649, and CVE-2015-8650.
CVE-2015-8649	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, and CVE-2015-8650.
CVE-2015-8650	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different

	vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, and CVE-2015-8649.
CVE-2015-8651	Integer overflow in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-8652	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, CVE-2015-8455, CVE-2015-8654, CVE-2015-8656, CVE-2015-8657, CVE-2015-8658, and CVE-2015-8820.
CVE-2015-8653	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted MPEG-4 data, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452,

	CVE-2015-8454, CVE-2015-8655, CVE-2015-8821, and CVE-2015-8822.
CVE-2015-8654	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, CVE-2015-8455, CVE-2015-8652, CVE-2015-8656, CVE-2015-8657, CVE-2015-8658, and CVE-2015-8820.
CVE-2015-8655	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted MPEG-4 data, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, CVE-2015-8454, CVE-2015-8653, CVE-2015-8821, and CVE-2015-8822.
CVE-2015-8656	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data, a different vulnerability than

	CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, CVE-2015-8455, CVE-2015-8652, CVE-2015-8654, CVE-2015-8657, CVE-2015-8658, and CVE-2015-8820.
CVE-2015-8657	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, CVE-2015-8455, CVE-2015-8652, CVE-2015-8654, CVE-2015-8656, CVE-2015-8658, and CVE-2015-8820.
CVE-2015-8658	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (uninitialized pointer dereference and memory corruption) via crafted MPEG-4 data, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, CVE-2015-8455, CVE-2015-8652, CVE-2015-8654, CVE-2015-8656, CVE-2015-8657, and CVE-2015-8820.
CVE-2015-8664	Integer overflow in the WebCursor::Deserialize function in content/common/cursors/webcursor.cc in Google Chrome before 47.0.2526.106 allows remote attackers to cause a denial of service or possibly have unspecified other impact via an RGBA pixel array with crafted dimensions, a different vulnerability than CVE-2015-6792.
CVE-2015-8820	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417,

	CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, CVE-2015-8455, CVE-2015-8652, CVE-2015-8654, CVE-2015-8656, CVE-2015-8657, and CVE-2015-8658.
CVE-2015-8821	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted MPEG-4 data, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, CVE-2015-8454, CVE-2015-8653, CVE-2015-8655, and CVE-2015-8822.
CVE-2015-8822	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted MPEG-4 data, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426,

	CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, CVE-2015-8454, CVE-2015-8653, CVE-2015-8655, and CVE-2015-8821.
CVE-2015-8823	Use-after-free vulnerability in the TextField object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted text property, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, CVE-2015-8454, CVE-2015-8653, CVE-2015-8655, CVE-2015-8821, and CVE-2015-8822.
CVE-2016-0959	Use after free vulnerability in Adobe Flash Player Desktop Runtime before 20.0.0.267, Adobe Flash Player Extended Support Release before 18.0.0.324, Adobe Flash Player for Google Chrome before 20.0.0.267, Adobe Flash Player for Microsoft Edge and Internet Explorer 11 before 20.0.0.267, Adobe Flash Player for Internet Explorer 10 and 11 before 20.0.0.267, Adobe Flash Player for Linux before 11.2.202.559, AIR Desktop Runtime before 20.0.0.233, AIR SDK before 20.0.0.233, AIR SDK & Compiler before 20.0.0.233, AIR for Android before 20.0.0.233.
CVE-2016-0960	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before

	21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.
CVE-2016-0961	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.
CVE-2016-0962	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.
CVE-2016-0963	Integer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0993 and CVE-2016-1010.
CVE-2016-0964	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.

CVE-2016-0965	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.
CVE-2016-0966	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.
CVE-2016-0967	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.
CVE-2016-0968	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.

CVE-2016-0969	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.
CVE-2016-0970	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.
CVE-2016-0971	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2016-0972	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.
CVE-2016-0973	Use-after-free vulnerability in the URLRequest object implementation in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before

	20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via a URLLoader.load call, a different vulnerability than CVE-2016-0974, CVE-2016-0975, CVE-2016-0982, CVE-2016-0983, and CVE-2016-0984.
CVE-2016-0974	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0973, CVE-2016-0975, CVE-2016-0982, CVE-2016-0983, and CVE-2016-0984.
CVE-2016-0975	Use-after-free vulnerability in the instanceof function in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code by leveraging improper reference handling, a different vulnerability than CVE-2016-0973, CVE-2016-0974, CVE-2016-0982, CVE-2016-0983, and CVE-2016-0984.
CVE-2016-0976	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.
CVE-2016-0977	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976,

	CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.
CVE-2016-0978	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.
CVE-2016-0979	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0980, and CVE-2016-0981.
CVE-2016-0980	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, and CVE-2016-0981.
CVE-2016-0981	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976,

	CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, and CVE-2016-0980.
CVE-2016-0982	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0973, CVE-2016-0974, CVE-2016-0975, CVE-2016-0983, and CVE-2016-0984.
CVE-2016-0983	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0973, CVE-2016-0974, CVE-2016-0975, CVE-2016-0982, and CVE-2016-0984.
CVE-2016-0984	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0973, CVE-2016-0974, CVE-2016-0975, CVE-2016-0982, and CVE-2016-0983.
CVE-2016-0985	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion."
CVE-2016-0986	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0962, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.

CVE-2016-0987	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.
CVE-2016-0988	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.
CVE-2016-0989	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.
CVE-2016-0990	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.
CVE-2016-0991	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before

	21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.
CVE-2016-0992	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-1002, and CVE-2016-1005.
CVE-2016-0993	Integer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0963 and CVE-2016-1010.
CVE-2016-0994	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code by using the actionCallMethod opcode with crafted arguments, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.
CVE-2016-0995	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.

CVE-2016-0996	Use-after-free vulnerability in the setInterval method in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via crafted arguments, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.
CVE-2016-0997	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.
CVE-2016-0998	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0999, and CVE-2016-1000.
CVE-2016-0999	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, and CVE-2016-1000.
CVE-2016-1000	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and

	before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, and CVE-2016-0999.
CVE-2016-1001	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2016-1002	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, and CVE-2016-1005.
CVE-2016-1005	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (uninitialized pointer dereference and memory corruption) via crafted MPEG-4 data, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, and CVE-2016-1002.
CVE-2016-1006	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to bypass the ASLR protection mechanism via JIT data.
CVE-2016-1010	Integer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0963 and CVE-2016-0993.

CVE-2016-1011	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1013, CVE-2016-1016, CVE-2016-1017, and CVE-2016-1031.
CVE-2016-1012	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1013	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1011, CVE-2016-1016, CVE-2016-1017, and CVE-2016-1031.
CVE-2016-1014	Untrusted search path vulnerability in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows local users to gain privileges via a Trojan horse resource in an unspecified directory.
CVE-2016-1015	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code by overriding NetConnection object properties to leverage an unspecified "type confusion," a different vulnerability than CVE-2016-1019.
CVE-2016-1016	Use-after-free vulnerability in the Transform object implementation in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via a flash.geom.Matrix callback, a different vulnerability than CVE-2016-1011, CVE-2016-1013, CVE-2016-1017, and CVE-2016-1031.
CVE-2016-1017	Use-after-free vulnerability in the LoadVars.decode function in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than

	CVE-2016-1011, CVE-2016-1013, CVE-2016-1016, and CVE-2016-1031.
CVE-2016-1018	Stack-based buffer overflow in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via crafted JPEG-XR data.
CVE-2016-1019	Adobe Flash Player 21.0.0.197 and earlier allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unspecified vectors, as exploited in the wild in April 2016.
CVE-2016-1020	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1021	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1022	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1023	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027,

	CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1024	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1025	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1026	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1027	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1028	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026,

	CVE-2016-1027, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1029	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1030	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to bypass intended access restrictions via unspecified vectors.
CVE-2016-1031	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1011, CVE-2016-1013, CVE-2016-1016, and CVE-2016-1017.
CVE-2016-1032	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, and CVE-2016-1033.
CVE-2016-1033	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, and CVE-2016-1032.
CVE-2016-1096	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.

CVE-2016-1097	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1098	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1099	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1100	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1101	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1102	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1103	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1104	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1105	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash

	libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1106	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1107	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1108	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1109	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1110	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1612	The LoadIC::UpdateCaches function in ic/ic.cc in Google V8, as used in Google Chrome before 48.0.2564.82, does not ensure receiver compatibility before performing a cast of an unspecified variable, which allows remote attackers to cause a denial of service or possibly have unknown other impact via crafted JavaScript code.
CVE-2016-1613	Multiple use-after-free vulnerabilities in the formfiller implementation in PDFium, as used in Google Chrome before 48.0.2564.82, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document, related to improper tracking of the destruction of (1) IPWL_FocusHandler and (2) IPWL_Provider objects.
CVE-2016-1614	The UnacceleratedImageBufferSurface class in WebKit/Source/platform/graphics/

	UnacceleratedImageBufferSurface.cpp in Blink, as used in Google Chrome before 48.0.2564.82, mishandles the initialization mode, which allows remote attackers to obtain sensitive information from process memory via a crafted web site.
CVE-2016-1615	The Omnibox implementation in Google Chrome before 48.0.2564.82 allows remote attackers to spoof a document's origin via unspecified vectors.
CVE-2016-1616	The CustomButton::AcceleratorPressed function in ui/views/controls/button/custom_button.cc in Google Chrome before 48.0.2564.82 allows remote attackers to spoof URLs via vectors involving an unfocused custom button.
CVE-2016-1617	The CSPSource::schemeMatches function in WebKit/Source/core/frame/csp/CSPSource.cpp in the Content Security Policy (CSP) implementation in Blink, as used in Google Chrome before 48.0.2564.82, does not apply http policies to https URLs and does not apply ws policies to wss URLs, which makes it easier for remote attackers to determine whether a specific HSTS web site has been visited by reading a CSP report.
CVE-2016-1618	Blink, as used in Google Chrome before 48.0.2564.82, does not ensure that a proper cryptographicallyRandomValues random number generator is used, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors.
CVE-2016-1619	Multiple integer overflows in the (1) sycc422_to_rgb and (2) sycc444_to_rgb functions in fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 48.0.2564.82, allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted PDF document.
CVE-2016-1620	Multiple unspecified vulnerabilities in Google Chrome before 48.0.2564.82 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1622	The Extensions subsystem in Google Chrome before 48.0.2564.109 does not prevent use of the Object.defineProperty method to override intended extension behavior, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.
CVE-2016-1623	The DOM implementation in Google Chrome before 48.0.2564.109 does not properly restrict frame-attach operations from occurring during or after frame-detach operations, which allows remote attackers to bypass the Same Origin Policy via a crafted web site, related

	to FrameLoader.cpp, HTMLFrameOwnerElement.h, LocalFrame.cpp, and WebLocalFrameImpl.cpp.
CVE-2016-1624	Integer underflow in the ProcessCommandsInternal function in dec/decode.c in Brotli, as used in Google Chrome before 48.0.2564.109, allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted data with brotli compression.
CVE-2016-1625	The Chrome Instant feature in Google Chrome before 48.0.2564.109 does not ensure that a New Tab Page (NTP) navigation target is on the most-visited or suggestions list, which allows remote attackers to bypass intended restrictions via unspecified vectors, related to instant_service.cc and search_tab_helper.cc.
CVE-2016-1626	The opj_pi_update_decode_poc function in pi.c in OpenJPEG, as used in PDFium in Google Chrome before 48.0.2564.109, miscalculates a certain layer index value, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document.
CVE-2016-1627	The Developer Tools (aka DevTools) subsystem in Google Chrome before 48.0.2564.109 does not validate URL schemes and ensure that the remoteBase parameter is associated with a chrome-devtools-frontend.appspot.com URL, which allows remote attackers to bypass intended access restrictions via a crafted URL, related to browser/devtools/devtools_ui_bindings.cc and WebKit/Source/devtools/front_end/Runtime.js.
CVE-2016-1628	pi.c in OpenJPEG, as used in PDFium in Google Chrome before 48.0.2564.109, does not validate a certain precision value, which allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via a crafted JPEG 2000 image in a PDF document, related to the opj_pi_next_rpcl, opj_pi_next_pcrl, and opj_pi_next_cprl functions.
CVE-2016-1629	Google Chrome before 48.0.2564.116 allows remote attackers to bypass the Blink Same Origin Policy and a sandbox protection mechanism via unspecified vectors.
CVE-2016-1630	The ContainerNode::parserRemoveChild function in WebKit/Source/core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 49.0.2623.75, mishandles widget updates, which makes it easier for remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1631	The PPB_Flash_MessageLoop_Impl::InternalRun function in content/renderer/pepper/ppb_flash_message_loop_impl.cc in the Pepper plugin in Google Chrome before 49.0.2623.75 mishandles

	nested message loops, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1632	The Extensions subsystem in Google Chrome before 49.0.2623.75 does not properly maintain own properties, which allows remote attackers to bypass intended access restrictions via crafted JavaScript code that triggers an incorrect cast, related to extensions/renderer/v8_helpers.h and gin/converter.h.
CVE-2016-1633	Use-after-free vulnerability in Blink, as used in Google Chrome before 49.0.2623.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2016-1634	Use-after-free vulnerability in the StyleResolver::appendCSSStyleSheet function in WebKit/Source/core/css/resolver/StyleResolver.cpp in Blink, as used in Google Chrome before 49.0.2623.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site that triggers Cascading Style Sheets (CSS) style invalidation during a certain subtree-removal action.
CVE-2016-1635	extensions/renderer/render_frame_observer_natives.cc in Google Chrome before 49.0.2623.75 does not properly consider object lifetimes and re-entrancy issues during OnDocumentElementCreated handling, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors.
CVE-2016-1636	The PendingScript::notifyFinished function in WebKit/Source/core/dom/PendingScript.cpp in Google Chrome before 49.0.2623.75 relies on memory-cache information about integrity-check occurrences instead of integrity-check successes, which allows remote attackers to bypass the Subresource Integrity (aka SRI) protection mechanism by triggering two loads of the same resource.
CVE-2016-1637	The SkATan2_255 function in effects/gradients/SkSweepGradient.cpp in Skia, as used in Google Chrome before 49.0.2623.75, mishandles arctangent calculations, which allows remote attackers to obtain sensitive information via a crafted web site.
CVE-2016-1638	extensions/renderer/resources/platform_app.js in the Extensions subsystem in Google Chrome before 49.0.2623.75 does not properly restrict use of Web APIs, which allows remote attackers to bypass intended access restrictions via a crafted platform app.
CVE-2016-1639	Use-after-free vulnerability in browser/extensions/api/webrtc_audio_private/webrtc_audio_private_api.cc in the WebRTC Audio Private API implementation in Google Chrome before 49.0.2623.75 allows remote

	attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect reliance on the resource context pointer.
CVE-2016-1640	The Web Store inline-installer implementation in the Extensions UI in Google Chrome before 49.0.2623.75 does not block installations upon deletion of an installation frame, which makes it easier for remote attackers to trick a user into believing that an installation request originated from the user's next navigation target via a crafted web site.
CVE-2016-1641	Use-after-free vulnerability in content/browser/web_contents/web_contents_impl.cc in Google Chrome before 49.0.2623.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering an image download after a certain data structure is deleted, as demonstrated by a favicon.ico download.
CVE-2016-1642	Multiple unspecified vulnerabilities in Google Chrome before 49.0.2623.75 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1643	The ImageInputType::ensurePrimaryContent function in WebKit/Source/core/html/forms/ImageInputType.cpp in Blink, as used in Google Chrome before 49.0.2623.87, does not properly maintain the user agent shadow DOM, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2016-1644	WebKit/Source/core/layout/LayoutObject.cpp in Blink, as used in Google Chrome before 49.0.2623.87, does not properly restrict relayout scheduling, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted HTML document.
CVE-2016-1645	Multiple integer signedness errors in the opj_j2k_update_image_data function in j2k.c in OpenJPEG, as used in PDFium in Google Chrome before 49.0.2623.87, allow remote attackers to cause a denial of service (incorrect cast and out-of-bounds write) or possibly have unspecified other impact via crafted JPEG 2000 data.
CVE-2016-1646	The Array.prototype.concat implementation in builtins.cc in Google V8, as used in Google Chrome before 49.0.2623.108, does not properly consider element data types, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-1647	Use-after-free vulnerability in the RenderWidgetHostImpl::Destroy function in content/

	browser/renderer_host/render_widget_host_impl.cc in the Navigation implementation in Google Chrome before 49.0.2623.108 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2016-1648	Use-after-free vulnerability in the GetLoadTimes function in renderer/loadtimes_extension_bindings.cc in the Extensions implementation in Google Chrome before 49.0.2623.108 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-1649	The Program::getUniformInternal function in Program.cpp in libANGLE, as used in Google Chrome before 49.0.2623.108, does not properly handle a certain data-type mismatch, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted shader stages.
CVE-2016-1650	The PageCaptureSaveAsMHTMLFunction::ReturnFailure function in browser/extensions/api/page_capture/page_capture_api.cc in Google Chrome before 49.0.2623.108 allows attackers to cause a denial of service or possibly have unspecified other impact by triggering an error in creating an MHTML document.
CVE-2016-1651	fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 50.0.2661.75, does not properly implement the sycc420_to_rgb and sycc422_to_rgb functions, which allows remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via crafted JPEG 2000 data in a PDF document.
CVE-2016-1652	Cross-site scripting (XSS) vulnerability in the ModuleSystem::RequireForJsInner function in extensions/renderer/module_system.cc in the Extensions subsystem in Google Chrome before 50.0.2661.75 allows remote attackers to inject arbitrary web script or HTML via a crafted web site, aka "Universal XSS (UXSS)."
CVE-2016-1653	The LoadBuffer implementation in Google V8, as used in Google Chrome before 50.0.2661.75, mishandles data types, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers an out-of-bounds write operation, related to compiler/pipeline.cc and compiler/simplified-lowering.cc.
CVE-2016-1654	The media subsystem in Google Chrome before 50.0.2661.75 does not initialize an unspecified data structure, which allows remote attackers to cause a

	denial of service (invalid read operation) via unknown vectors.
CVE-2016-1655	Google Chrome before 50.0.2661.75 does not properly consider that frame removal may occur during callback execution, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted extension.
CVE-2016-1657	The WebContentsImpl::FocusLocationBarByDefault function in content/browser/web_contents/web_contents_impl.cc in Google Chrome before 50.0.2661.75 mishandles focus for certain about:blank pages, which allows remote attackers to spoof the address bar via a crafted URL.
CVE-2016-1658	The Extensions subsystem in Google Chrome before 50.0.2661.75 incorrectly relies on GetOrigin method calls for origin comparisons, which allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted extension.
CVE-2016-1659	Multiple unspecified vulnerabilities in Google Chrome before 50.0.2661.75 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1660	Blink, as used in Google Chrome before 50.0.2661.94, mishandles assertions in the WTF::BitArray and WTF::double_conversion::Vector classes, which allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via a crafted web site.
CVE-2016-1661	Blink, as used in Google Chrome before 50.0.2661.94, does not ensure that frames satisfy a check for the same renderer process in addition to a Same Origin Policy check, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted web site, related to BindingSecurity.cpp and DOMWindow.cpp.
CVE-2016-1662	extensions/renderer/gc_callback.cc in Google Chrome before 50.0.2661.94 does not prevent fallback execution once the Garbage Collection callback has started, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors.
CVE-2016-1663	The SerializedScriptValue::transferArrayBuffers function in WebKit/Source/bindings/core/v8/SerializedScriptValue.cpp in the V8 bindings in Blink, as used in Google Chrome before 50.0.2661.94, mishandles certain array-buffer data structures, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site.

CVE-2016-1664	The HistoryController::UpdateForCommit function in content/renderer/history_controller.cc in Google Chrome before 50.0.2661.94 mishandles the interaction between subframe forward navigations and other forward navigations, which allows remote attackers to spoof the address bar via a crafted web site.
CVE-2016-1665	The JSGenericLowering class in compiler/js-generic-lowering.cc in Google V8, as used in Google Chrome before 50.0.2661.94, mishandles comparison operators, which allows remote attackers to obtain sensitive information via crafted JavaScript code.
CVE-2016-1666	Multiple unspecified vulnerabilities in Google Chrome before 50.0.2661.94 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1667	The TreeScope::adoptIfNeeded function in WebKit/Source/core/dom/TreeScope.cpp in the DOM implementation in Blink, as used in Google Chrome before 50.0.2661.102, does not prevent script execution during node-adoption operations, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1668	The forEachForBinding function in WebKit/Source/bindings/core/v8/Iterable.h in the V8 bindings in Blink, as used in Google Chrome before 50.0.2661.102, uses an improper creation context, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1669	The Zone::New function in zone.cc in Google V8 before 5.0.71.47, as used in Google Chrome before 50.0.2661.102, does not properly determine when to expand certain memory allocations, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-1670	Race condition in the ResourceDispatcherHostImpl::BeginRequest function in content/browser/loader/resource_dispatcher_host_impl.cc in Google Chrome before 50.0.2661.102 allows remote attackers to make arbitrary HTTP requests by leveraging access to a renderer process and reusing a request ID.
CVE-2016-1672	The ModuleSystem::RequireForJsInner function in extensions/renderer/module_system.cc in the extension bindings in Google Chrome before 51.0.2704.63 mishandles properties, which allows remote attackers to conduct bindings-interception attacks and bypass the Same Origin Policy via unspecified vectors.

CVE-2016-1673	Blink, as used in Google Chrome before 51.0.2704.63, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2016-1674	The extensions subsystem in Google Chrome before 51.0.2704.63 allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2016-1675	Blink, as used in Google Chrome before 51.0.2704.63, allows remote attackers to bypass the Same Origin Policy by leveraging the mishandling of Document reattachment during destruction, related to FrameLoader.cpp and LocalFrame.cpp.
CVE-2016-1676	extensions/renderer/resources/binding.js in the extension bindings in Google Chrome before 51.0.2704.63 does not properly use prototypes, which allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2016-1677	uri.js in Google V8 before 5.1.281.26, as used in Google Chrome before 51.0.2704.63, uses an incorrect array type, which allows remote attackers to obtain sensitive information by calling the decodeURI function and leveraging "type confusion."
CVE-2016-1678	objects.cc in Google V8 before 5.0.71.32, as used in Google Chrome before 51.0.2704.63, does not properly restrict lazy deoptimization, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-1679	The ToV8Value function in content/child/v8_value_converter_impl.cc in the V8 bindings in Google Chrome before 51.0.2704.63 does not properly restrict use of getters and setters, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-1680	Use-after-free vulnerability in ports/SkFontHost_FreeType.cpp in Skia, as used in Google Chrome before 51.0.2704.63, allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2016-1681	Heap-based buffer overflow in the opj_j2k_read_SPCod_SPCoc function in j2k.c in OpenJPEG, as used in PDFium in Google Chrome before 51.0.2704.63, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.
CVE-2016-1682	The ServiceWorkerContainer::registerServiceWorkerImpl function in WebKit/Source/modules/serviceworkers/ServiceWorkerContainer.cpp in Blink, as used in

	Google Chrome before 51.0.2704.63, allows remote attackers to bypass the Content Security Policy (CSP) protection mechanism via a ServiceWorker registration.
CVE-2016-1683	numbers.c in libxslt before 1.1.29, as used in Google Chrome before 51.0.2704.63, mishandles namespace nodes, which allows remote attackers to cause a denial of service (out-of-bounds heap memory access) or possibly have unspecified other impact via a crafted document.
CVE-2016-1684	numbers.c in libxslt before 1.1.29, as used in Google Chrome before 51.0.2704.63, mishandles the i format token for xsl:number data, which allows remote attackers to cause a denial of service (integer overflow or resource consumption) or possibly have unspecified other impact via a crafted document.
CVE-2016-1685	core/fxge/ge/fx_ge_text.cpp in PDFium, as used in Google Chrome before 51.0.2704.63, miscalculates certain index values, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document.
CVE-2016-1686	The CPDF_DIBSource::CreateDecoder function in core/fpdfapi/fpdf_render/fpdf_render_loadimage.cpp in PDFium, as used in Google Chrome before 51.0.2704.63, mishandles decoder-initialization failure, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document.
CVE-2016-1687	The renderer implementation in Google Chrome before 51.0.2704.63 does not properly restrict public exposure of classes, which allows remote attackers to obtain sensitive information via vectors related to extensions.
CVE-2016-1688	The regexp (aka regular expression) implementation in Google V8 before 5.0.71.40, as used in Google Chrome before 51.0.2704.63, mishandles external string sizes, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted JavaScript code.
CVE-2016-1689	Heap-based buffer overflow in content/renderer/media/canvas_capture_handler.cc in Google Chrome before 51.0.2704.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site.
CVE-2016-1690	The Autofill implementation in Google Chrome before 51.0.2704.63 mishandles the interaction between field updates and JavaScript code that triggers a frame deletion, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site, a different vulnerability than CVE-2016-1701.

CVE-2016-1691	Skia, as used in Google Chrome before 51.0.2704.63, mishandles coincidence runs, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted curves, related to SkOpCoincidence.cpp and SkPathOpsCommon.cpp.
CVE-2016-1692	WebKit/Source/core/css/StyleSheetContents.cpp in Blink, as used in Google Chrome before 51.0.2704.63, permits cross-origin loading of CSS stylesheets by a ServiceWorker even when the stylesheet download has an incorrect MIME type, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1693	browser/safe_browsing/srt_field_trial_win.cc in Google Chrome before 51.0.2704.63 does not use the HTTPS service on dl.google.com to obtain the Software Removal Tool, which allows remote attackers to spoof the chrome_cleanup_tool.exe (aka CCT) file via a man-in-the-middle attack on an HTTP session.
CVE-2016-1694	browser/browsing_data/browsing_data_remover.cc in Google Chrome before 51.0.2704.63 deletes HPKP pins during cache clearing, which makes it easier for remote attackers to spoof web sites via a valid certificate from an arbitrary recognized Certification Authority.
CVE-2016-1695	Multiple unspecified vulnerabilities in Google Chrome before 51.0.2704.63 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1696	The extensions subsystem in Google Chrome before 51.0.2704.79 does not properly restrict bindings access, which allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2016-1697	The FrameLoader::startLoad function in WebKit/Source/core/loader/FrameLoader.cpp in Blink, as used in Google Chrome before 51.0.2704.79, does not prevent frame navigations during DocumentLoader detach operations, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.
CVE-2016-1698	The createCustomType function in extensions/renderer/resources/binding.js in the extension bindings in Google Chrome before 51.0.2704.79 does not validate module types, which might allow attackers to load arbitrary modules or obtain sensitive information by leveraging a poisoned definition.
CVE-2016-1699	WebKit/Source/devtools/front_end/devtools.js in the Developer Tools (aka DevTools) subsystem in Blink, as used in Google Chrome before 51.0.2704.79, does not ensure that the remoteFrontendUrl parameter is associated with a chrome-devtools-frontend.appspot.com URL, which allows remote

	attackers to bypass intended access restrictions via a crafted URL.
CVE-2016-1700	extensions/renderer/runtime_custom_bindings.cc in Google Chrome before 51.0.2704.79 does not consider side effects during creation of an array of extension views, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to extensions.
CVE-2016-1701	The Autofill implementation in Google Chrome before 51.0.2704.79 mishandles the interaction between field updates and JavaScript code that triggers a frame deletion, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site, a different vulnerability than CVE-2016-1690.
CVE-2016-1702	The SkRegion::readFromMemory function in core/SkRegion.cpp in Skia, as used in Google Chrome before 51.0.2704.79, does not validate the interval count, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted serialized data.
CVE-2016-1703	Multiple unspecified vulnerabilities in Google Chrome before 51.0.2704.79 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1704	Multiple unspecified vulnerabilities in Google Chrome before 51.0.2704.103 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1705	Multiple unspecified vulnerabilities in Google Chrome before 52.0.2743.82 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1706	The PPAPI implementation in Google Chrome before 52.0.2743.82 does not validate the origin of IPC messages to the plugin broker process that should have come from the browser process, which allows remote attackers to bypass a sandbox protection mechanism via an unexpected message type, related to broker_process_dispatcher.cc, ppapi_plugin_process_host.cc, ppapi_thread.cc, and render_frame_message_filter.cc.
CVE-2016-1707	ios/web/web_state/ui/crw_web_controller.mm in Google Chrome before 52.0.2743.82 on iOS does not ensure that an invalid URL is replaced with the about:blank URL, which allows remote attackers to spoof the URL display via a crafted web site.
CVE-2016-1708	The Chrome Web Store inline-installation implementation in the Extensions subsystem in Google Chrome before 52.0.2743.82 does not properly

	consider object lifetimes during progress observation, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site.
CVE-2016-1709	Heap-based buffer overflow in the ByteArray::Get method in data/byte_array.cc in Google sfntly before 2016-06-10, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted SFNT font.
CVE-2016-1710	The ChromeClientImpl::createWindow method in WebKit/Source/web/ChromeClientImpl.cpp in Blink, as used in Google Chrome before 52.0.2743.82, does not prevent window creation by a deferred frame, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1711	WebKit/Source/core/loader/FrameLoader.cpp in Blink, as used in Google Chrome before 52.0.2743.82, does not disable frame navigation during a detach operation on a DocumentLoader object, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-2051	Multiple unspecified vulnerabilities in Google V8 before 4.8.271.17, as used in Google Chrome before 48.0.2564.82, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-2052	Multiple unspecified vulnerabilities in HarfBuzz before 1.0.6, as used in Google Chrome before 48.0.2564.82, allow attackers to cause a denial of service or possibly have other impact via crafted data, as demonstrated by a buffer over-read resulting from an inverted length check in hb-ot-font.cc, a different issue than CVE-2015-8947.
CVE-2016-2843	Multiple unspecified vulnerabilities in Google V8 before 4.9.385.26, as used in Google Chrome before 49.0.2623.75, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-2844	WebKit/Source/core/layout/LayoutBlock.cpp in Blink, as used in Google Chrome before 49.0.2623.75, does not properly determine when anonymous block wrappers may exist, which allows remote attackers to cause a denial of service (incorrect cast and assertion failure) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-2845	The Content Security Policy (CSP) implementation in Blink, as used in Google Chrome before 49.0.2623.75, does not ignore a URL's path component in the case of a ServiceWorker fetch, which allows remote attackers

	to obtain sensitive information about visited web pages by reading CSP violation reports, related to FrameFetchContext.cpp and ResourceFetcher.cpp.
CVE-2016-3508	Unspecified vulnerability in Oracle Java SE 6u115, 7u101, and 8u92; Java SE Embedded 8u91; and JRockit R28.3.10 allows remote attackers to affect availability via vectors related to JAXP, a different vulnerability than CVE-2016-3500.
CVE-2016-3550	Unspecified vulnerability in Oracle Java SE 6u115, 7u101, and 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality via vectors related to Hotspot.
CVE-2016-3587	Unspecified vulnerability in Oracle Java SE 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot.
CVE-2016-3598	Unspecified vulnerability in Oracle Java SE 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Libraries, a different vulnerability than CVE-2016-3610.
CVE-2016-3606	Unspecified vulnerability in Oracle Java SE 7u101 and 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot.
CVE-2016-3610	Unspecified vulnerability in Oracle Java SE 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Libraries, a different vulnerability than CVE-2016-3598.
CVE-2016-3679	Multiple unspecified vulnerabilities in Google V8 before 4.9.385.33, as used in Google Chrome before 49.0.2623.108, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-4108	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4109	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4110	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash

	libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4111	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4112	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4113	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4114	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4115	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4116	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4117	Adobe Flash Player 21.0.0.226 and earlier allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in May 2016.
CVE-2016-4120	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098,

	CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4160, CVE-2016-4161, CVE-2016-4162, and CVE-2016-4163.
CVE-2016-4121	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1097, CVE-2016-1106, CVE-2016-1107, CVE-2016-1108, CVE-2016-1109, CVE-2016-1110, CVE-2016-4108, and CVE-2016-4110.
CVE-2016-4122	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4123	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4124	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4125	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4127	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4128	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.

CVE-2016-4129	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4130	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4131	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4132	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4133	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4134	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4135	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4136	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4137	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash

	libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4138	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4139	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4140	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4141	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4142	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4143	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4144	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4145	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack

	vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4146	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4147	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4148	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4149	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4150	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4151	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4152	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4153	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.

CVE-2016-4154	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4155	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4156	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4160	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4120, CVE-2016-4161, CVE-2016-4162, and CVE-2016-4163.
CVE-2016-4161	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4120, CVE-2016-4160, CVE-2016-4162, and CVE-2016-4163.
CVE-2016-4162	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4120, CVE-2016-4160, CVE-2016-4161, and CVE-2016-4163.

CVE-2016-4163	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4120, CVE-2016-4160, CVE-2016-4161, and CVE-2016-4162.
CVE-2016-4166	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4171	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier allows remote attackers to execute arbitrary code via unknown vectors, as exploited in the wild in June 2016.
CVE-2016-4172	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4173	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4174	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute

	arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4175	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4176	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4177.
CVE-2016-4177	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4176.
CVE-2016-4178	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors.
CVE-2016-4179	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233,

	CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4180	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4181	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4182	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236,

	CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4183	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4184	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4185	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239,

	CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4186	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4187	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4188	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242,

	CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4189	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4190	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4217	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242,

	CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4218	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4219	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4220	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242,

	CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4221	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4222	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4223	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2016-4224 and CVE-2016-4225.
CVE-2016-4224	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2016-4223 and CVE-2016-4225.
CVE-2016-4225	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2016-4223 and CVE-2016-4224.
CVE-2016-4226	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different

	vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4227	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4228	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4229	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4230	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4231	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, and CVE-2016-4248.
CVE-2016-4232	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and

	before 11.2.202.632 on Linux allows attackers to obtain sensitive information from process memory via unspecified vectors.
CVE-2016-4233	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4234	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4235	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242,

	CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4236	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4237	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4238	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242,

	CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4239	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4240	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4241	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4242,

	CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4242	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4243	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4244	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241,

	CVE-2016-4242, CVE-2016-4243, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4245	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, and CVE-2016-4246.
CVE-2016-4246	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, and CVE-2016-4245.
CVE-2016-4247	Race condition in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to obtain sensitive information via unspecified vectors.
CVE-2016-4248	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, and CVE-2016-4231.

CVE-2016-4249	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2016-4271	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2016-4277 and CVE-2016-4278, aka a "local-with-filesystem Flash sandbox bypass" issue.
CVE-2016-4272	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932.
CVE-2016-4273	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, CVE-2016-6989, and CVE-2016-6990.
CVE-2016-4274	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.
CVE-2016-4275	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.
CVE-2016-4276	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to

	execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.
CVE-2016-4277	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2016-4271 and CVE-2016-4278.
CVE-2016-4278	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2016-4271 and CVE-2016-4277.
CVE-2016-4279	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932.
CVE-2016-4280	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.
CVE-2016-4281	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.
CVE-2016-4282	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275,

	CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.
CVE-2016-4283	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4284, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.
CVE-2016-4284	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.
CVE-2016-4285	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-6922, and CVE-2016-6924.
CVE-2016-4286	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to bypass intended access restrictions via unspecified vectors.
CVE-2016-4287	Integer overflow in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2016-5127	Use-after-free vulnerability in WebKit/Source/core/editing/VisibleUnits.cpp in Blink, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code involving an @import at-rule in a Cascading Style Sheets (CSS) token sequence in conjunction with a rel=import attribute of a LINK element.
CVE-2016-5128	objects.cc in Google V8 before 5.2.361.27, as used in Google Chrome before 52.0.2743.82, does not prevent API interceptors from modifying a store target without

	setting a property, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-5129	Google V8 before 5.2.361.32, as used in Google Chrome before 52.0.2743.82, does not properly process left-trimmed objects, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-5130	content/renderer/history_controller.cc in Google Chrome before 52.0.2743.82 does not properly restrict multiple uses of a JavaScript forward method, which allows remote attackers to spoof the URL display via a crafted web site.
CVE-2016-5131	Use-after-free vulnerability in libxml2 through 2.9.4, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the XPointer range-to function.
CVE-2016-5132	The Service Workers subsystem in Google Chrome before 52.0.2743.82 does not properly implement the Secure Contexts specification during decisions about whether to control a subframe, which allows remote attackers to bypass the Same Origin Policy via an https IFRAME element inside an http IFRAME element.
CVE-2016-5133	Google Chrome before 52.0.2743.82 mishandles origin information during proxy authentication, which allows man-in-the-middle attackers to spoof a proxy-authentication login prompt or trigger incorrect credential storage by modifying the client-server data stream.
CVE-2016-5134	net/proxy/proxy_service.cc in the Proxy Auto-Config (PAC) feature in Google Chrome before 52.0.2743.82 does not ensure that URL information is restricted to a scheme, host, and port, which allows remote attackers to discover credentials by operating a server with a PAC script, a related issue to CVE-2016-3763.
CVE-2016-5135	WebKit/Source/core/html/parser/HTMLPreloadScanner.cpp in Blink, as used in Google Chrome before 52.0.2743.82, does not consider referrer-policy information inside an HTML document during a preload request, which allows remote attackers to bypass the Content Security Policy (CSP) protection mechanism via a crafted web site, as demonstrated by a "Content-Security-Policy: referrer origin-when-cross-origin" header that overrides a "<META name='referrer' content='no-referrer'>" element.
CVE-2016-5136	Use-after-free vulnerability in extensions/renderer/user_script_injector.cc in the Extensions subsystem in Google Chrome before 52.0.2743.82 allows remote attackers to cause a denial of service or possibly have

	unspecified other impact via vectors related to script deletion.
CVE-2016-5137	The CSPSource::schemeMatches function in WebKit/Source/core/frame/csp/CSPSource.cpp in the Content Security Policy (CSP) implementation in Blink, as used in Google Chrome before 52.0.2743.82, does not apply http :80 policies to https :443 URLs and does not apply ws :80 policies to wss :443 URLs, which makes it easier for remote attackers to determine whether a specific HSTS web site has been visited by reading a CSP report. NOTE: this vulnerability is associated with a specification change after CVE-2016-1617 resolution.
CVE-2016-5139	Multiple integer overflows in the opj_tcd_init_tile function in tcd.c in OpenJPEG, as used in PDFium in Google Chrome before 52.0.2743.116, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data.
CVE-2016-5140	Heap-based buffer overflow in the opj_j2k_read_SQcd_SQcc function in j2k.c in OpenJPEG, as used in PDFium in Google Chrome before 52.0.2743.116, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JPEG 2000 data.
CVE-2016-5141	Blink, as used in Google Chrome before 52.0.2743.116, allows remote attackers to spoof the address bar via vectors involving a provisional URL for an initially empty document, related to FrameLoader.cpp and ScopedPageLoadDeferrer.cpp.
CVE-2016-5142	The Web Cryptography API (aka WebCrypto) implementation in Blink, as used in Google Chrome before 52.0.2743.116, does not properly copy data buffers, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code, related to NormalizeAlgorithm.cpp and SubtleCrypto.cpp.
CVE-2016-5143	The Developer Tools (aka DevTools) subsystem in Blink, as used in Google Chrome before 52.0.2743.116, mishandles the script-path hostname, remoteBase parameter, and remoteFrontendUrl parameter, which allows remote attackers to bypass intended access restrictions via a crafted URL, a different vulnerability than CVE-2016-5144.
CVE-2016-5144	The Developer Tools (aka DevTools) subsystem in Blink, as used in Google Chrome before 52.0.2743.116, mishandles the script-path hostname, remoteBase parameter, and remoteFrontendUrl parameter, which allows remote attackers to bypass intended access restrictions via a crafted URL, a different vulnerability than CVE-2016-5143.

CVE-2016-5145	Blink, as used in Google Chrome before 52.0.2743.116, does not ensure that a taint property is preserved after a structure-clone operation on an ImageBitmap object derived from a cross-origin image, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.
CVE-2016-5146	Multiple unspecified vulnerabilities in Google Chrome before 52.0.2743.116 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-5147	Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, mishandles deferred page loads, which allows remote attackers to inject arbitrary web script or HTML via a crafted web site, aka "Universal XSS (UXSS)."
CVE-2016-5148	Cross-site scripting (XSS) vulnerability in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to inject arbitrary web script or HTML via vectors related to widget updates, aka "Universal XSS (UXSS)."
CVE-2016-5149	The extensions subsystem in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux relies on an IFRAME source URL to identify an associated extension, which allows remote attackers to conduct extension-bindings injection attacks by leveraging script access to a resource that initially has the about:blank URL.
CVE-2016-5150	WebKit/Source/bindings/modules/v8/V8BindingForModules.cpp in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, has an Indexed Database (aka IndexedDB) API implementation that does not properly restrict key-path evaluation, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code that leverages certain side effects.
CVE-2016-5151	PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux mishandles timers, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted PDF document, related to fpdfsdk/javascript/JS_Object.cpp and fpdfsdk/javascript/app.cpp.
CVE-2016-5152	Integer overflow in the opj_tcd_get_decoded_tile_size function in tcd.c in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to cause a denial of service (heap-

	based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data.
CVE-2016-5153	The Web Animations implementation in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, improperly relies on list iteration, which allows remote attackers to cause a denial of service (use-after-destruction) or possibly have unspecified other impact via a crafted web site.
CVE-2016-5154	Multiple heap-based buffer overflows in PDFium, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted JBig2 image.
CVE-2016-5155	Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly validate access to the initial document, which allows remote attackers to spoof the address bar via a crafted web site.
CVE-2016-5156	extensions/renderer/event_bindings.cc in the event bindings in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux attempts to process filtered events after failure to add an event matcher, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors.
CVE-2016-5157	Heap-based buffer overflow in the opj_dwt_interleave_v function in dwt.c in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to execute arbitrary code via crafted coordinate values in JPEG 2000 data.
CVE-2016-5158	Multiple integer overflows in the opj_tcd_init_tile function in tcd.c in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data.
CVE-2016-5159	Multiple integer overflows in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data that is mishandled during opj_aligned_malloc calls in dwt.c and t1.c.
CVE-2016-5160	The AllowCrossRendererResourceLoad function in extensions/browser/url_request_util.cc in Google

	Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly use an extension's manifest.json web_accessible_resources field for restrictions on IFRAME elements, which makes it easier for remote attackers to conduct clickjacking attacks, and trick users into changing extension settings, via a crafted web site, a different vulnerability than CVE-2016-5162.
CVE-2016-5161	The EditingStyle::mergeStyle function in WebKit/Source/core/editing/EditingStyle.cpp in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, mishandles custom properties, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site that leverages "type confusion" in the StylePropertySerializer class.
CVE-2016-5162	The AllowCrossRendererResourceLoad function in extensions/browser/url_request_util.cc in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly use an extension's manifest.json web_accessible_resources field for restrictions on IFRAME elements, which makes it easier for remote attackers to conduct clickjacking attacks, and trick users into changing extension settings, via a crafted web site, a different vulnerability than CVE-2016-5160.
CVE-2016-5163	The bidirectional-text implementation in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not ensure left-to-right (LTR) rendering of URLs, which allows remote attackers to spoof the address bar via crafted right-to-left (RTL) Unicode text, related to omnibox/SuggestionView.java and omnibox/UrlBar.java in Chrome for Android.
CVE-2016-5164	Cross-site scripting (XSS) vulnerability in WebKit/Source/platform/v8_inspector/V8Debugger.cpp in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to inject arbitrary web script or HTML into the Developer Tools (aka DevTools) subsystem via a crafted web site, aka "Universal XSS (UXSS)."
CVE-2016-5165	Cross-site scripting (XSS) vulnerability in the Developer Tools (aka DevTools) subsystem in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux allows remote attackers to inject arbitrary web script or HTML via the settings parameter in a chrome-devtools-frontend.appspot.com URL's query string.
CVE-2016-5166	The download implementation in Google Chrome before 53.0.2785.89 on Windows and OS X and before

	53.0.2785.92 on Linux does not properly restrict saving a file:// URL that is referenced by an http:// URL, which makes it easier for user-assisted remote attackers to discover NetNTLM hashes and conduct SMB relay attacks via a crafted web page that is accessed with the "Save page as" menu choice.
CVE-2016-5167	Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-5168	Skia, as used in Google Chrome before 50.0.2661.94, allows remote attackers to bypass the Same Origin Policy and obtain sensitive information.
CVE-2016-5170	WebKit/Source/bindings/modules/v8/ V8BindingForModules.cpp in Blink, as used in Google Chrome before 53.0.2785.113, does not properly consider getter side effects during array key conversion, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted Indexed Database (aka IndexedDB) API calls.
CVE-2016-5171	WebKit/Source/bindings/templates/interface.cpp in Blink, as used in Google Chrome before 53.0.2785.113, does not prevent certain constructor calls, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-5172	The parser in Google V8, as used in Google Chrome before 53.0.2785.113, mishandles scopes, which allows remote attackers to obtain sensitive information from arbitrary memory locations via crafted JavaScript code.
CVE-2016-5173	The extensions subsystem in Google Chrome before 53.0.2785.113 does not properly restrict access to Object.prototype, which allows remote attackers to load unintended resources, and consequently trigger unintended JavaScript function calls and bypass the Same Origin Policy via an indirect interception attack.
CVE-2016-5174	browser/ui/cocoa/ browser_window_controller_private.mm in Google Chrome before 53.0.2785.113 does not process fullscreen toggle requests during a fullscreen transition, which allows remote attackers to cause a denial of service (unsuppressed popup) via a crafted web site.
CVE-2016-5175	Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.113 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.

CVE-2016-5176	Google Chrome before 53.0.2785.113 allows remote attackers to bypass the SafeBrowsing protection mechanism via unspecified vectors.
CVE-2016-5177	Use-after-free vulnerability in V8 in Google Chrome before 53.0.2785.143 allows remote attackers to cause a denial of service (crash) or possibly have unspecified other impact via unknown vectors.
CVE-2016-5178	Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.143 allow remote attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-5181	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android permitted execution of v8 microtasks while the DOM was in an inconsistent state, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages.
CVE-2016-5182	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android had insufficient validation in bitmap handling, which allowed a remote attacker to potentially exploit heap corruption via crafted HTML pages.
CVE-2016-5183	A heap use after free in PDFium in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android allows a remote attacker to potentially exploit heap corruption via crafted PDF files.
CVE-2016-5184	PDFium in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object lifecycles in CFFL_FormFillter::KillFocusForAnnot, which allowed a remote attacker to potentially exploit heap corruption via crafted PDF files.
CVE-2016-5185	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly allowed reentrance of FrameView::updateLifecyclePhasesInternal(), which allowed a remote attacker to perform an out of bounds memory read via crafted HTML pages.
CVE-2016-5186	Devtools in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled objects after a tab crash, which allowed a remote attacker to perform an out of bounds memory read via crafted PDF files.
CVE-2016-5187	Google Chrome prior to 54.0.2840.85 for Android incorrectly handled rapid transition into and out of full screen mode, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages.

CVE-2016-5188	Multiple issues in Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux allow a remote attacker to spoof various parts of browser UI via crafted HTML pages.
CVE-2016-5189	Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android permitted navigation to blob URLs with non-canonical origins, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages.
CVE-2016-5190	Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object lifecycles during shutdown, which allowed a remote attacker to perform an out of bounds memory read via crafted HTML pages.
CVE-2016-5191	Bookmark handling in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android had insufficient validation of supplied data, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages, as demonstrated by an interpretation conflict between userinfo and scheme in an http://javascript:payload@example.com URL.
CVE-2016-5192	Blink in Google Chrome prior to 54.0.2840.59 for Windows missed a CORS check on redirect in TextTrackLoader, which allowed a remote attacker to bypass cross-origin restrictions via crafted HTML pages.
CVE-2016-5193	Google Chrome prior to 54.0 for iOS had insufficient validation of URLs for windows open by DOM, which allowed a remote attacker to bypass restrictions on navigation to certain URL schemes via crafted HTML pages.
CVE-2016-5194	Unspecified vulnerabilities in Google Chrome before 54.0.2840.59.
CVE-2016-5198	V8 in Google Chrome prior to 54.0.2840.90 for Linux, and 54.0.2840.85 for Android, and 54.0.2840.87 for Windows and Mac included incorrect optimisation assumptions, which allowed a remote attacker to perform arbitrary read/write operations, leading to code execution, via a crafted HTML page.
CVE-2016-5199	An off by one error resulting in an allocation of zero size in FFmpeg in Google Chrome prior to 54.0.2840.98 for Mac, and 54.0.2840.99 for Windows, and 54.0.2840.100 for Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2016-5200	V8 in Google Chrome prior to 54.0.2840.98 for Mac, and 54.0.2840.99 for Windows, and 54.0.2840.100 for Linux, and 55.0.2883.84 for Android incorrectly applied type rules, which allowed a remote attacker to

	potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5201	A leak of privateClass in the extensions API in Google Chrome prior to 54.0.2840.100 for Linux, and 54.0.2840.99 for Windows, and 54.0.2840.98 for Mac allowed a remote attacker to access privileged JavaScript code via a crafted HTML page.
CVE-2016-5202	browser/extensions/api/dial/dial_registry.cc in Google Chrome before 54.0.2840.98 on macOS, before 54.0.2840.99 on Windows, and before 54.0.2840.100 on Linux neglects to copy a device ID before an erase() call, which causes the erase operation to access data that that erase operation will destroy.
CVE-2016-5203	A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2016-5204	Leaking of an SVG shadow tree leading to corruption of the DOM tree in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2016-5205	Blink in Google Chrome prior to 55.0.2883.75 for Linux, Windows and Mac, incorrectly handles deferred page loads, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2016-5206	The PDF plugin in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly followed redirects, which allowed a remote attacker to bypass the Same Origin Policy via a crafted HTML page.
CVE-2016-5207	In Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android, corruption of the DOM tree could occur during the removal of a full screen element, which allowed a remote attacker to achieve arbitrary code execution via a crafted HTML page.
CVE-2016-5208	Blink in Google Chrome prior to 55.0.2883.75 for Linux and Windows, and 55.0.2883.84 for Android allowed possible corruption of the DOM tree during synchronous event handling, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2016-5209	Bad casting in bitmap manipulation in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2016-5210	Heap buffer overflow during TIFF image parsing in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2016-5211	A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2016-5212	Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android insufficiently sanitized DevTools URLs, which allowed a remote attacker to read local files via a crafted HTML page.
CVE-2016-5213	A use after free in V8 in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5214	Google Chrome prior to 55.0.2883.75 for Windows mishandled downloaded files, which allowed a remote attacker to prevent the downloaded file from receiving the Mark of the Web via a crafted HTML page.
CVE-2016-5215	A use after free in webaudio in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2016-5216	A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2016-5217	The extensions API in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly permitted access to privileged plugins, which allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2016-5218	The extensions API in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled navigation within PDFs, which allowed a remote attacker to temporarily spoof the contents of the Omnibox (URL bar) via a crafted HTML page containing PDF data.
CVE-2016-5219	A heap use after free in V8 in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2016-5220	PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled navigation within PDFs, which allowed a remote attacker to read local files via a crafted PDF file.
CVE-2016-5221	Type confusion in libGLESv2 in ANGLE in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android possibly allowed a remote attacker to bypass buffer validation via a crafted HTML page.
CVE-2016-5222	Incorrect handling of invalid URLs in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2016-5223	Integer overflow in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption or DoS via a crafted PDF file.
CVE-2016-5224	A timing attack on denormalized floating point arithmetic in SVG filters in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to bypass the Same Origin Policy via a crafted HTML page.
CVE-2016-5225	Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled form actions, which allowed a remote attacker to bypass Content Security Policy via a crafted HTML page.
CVE-2016-5226	Blink in Google Chrome prior to 55.0.2883.75 for Linux, Windows and Mac executed javascript: URLs entered in the URL bar in the context of the current tab, which allowed a socially engineered user to XSS themselves by dragging and dropping a javascript: URL into the URL bar.
CVE-2016-6921	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932.
CVE-2016-6922	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service

	(memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, and CVE-2016-6924.
CVE-2016-6923	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932.
CVE-2016-6924	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, and CVE-2016-6922.
CVE-2016-6925	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932.
CVE-2016-6926	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932.
CVE-2016-6927	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932.

CVE-2016-6929	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932.
CVE-2016-6930	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6931, and CVE-2016-6932.
CVE-2016-6931	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, and CVE-2016-6932.
CVE-2016-6932	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6921, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, and CVE-2016-6931.
CVE-2016-6981	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-6987.
CVE-2016-6982	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4273, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, CVE-2016-6989, and CVE-2016-6990.

CVE-2016-6983	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4273, CVE-2016-6982, CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, CVE-2016-6989, and CVE-2016-6990.
CVE-2016-6984	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4273, CVE-2016-6982, CVE-2016-6983, CVE-2016-6985, CVE-2016-6986, CVE-2016-6989, and CVE-2016-6990.
CVE-2016-6985	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4273, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6986, CVE-2016-6989, and CVE-2016-6990.
CVE-2016-6986	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4273, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6989, and CVE-2016-6990.
CVE-2016-6987	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-6981.
CVE-2016-6989	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4273, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, and CVE-2016-6990.
CVE-2016-6990	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different

	vulnerability than CVE-2016-4273, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, and CVE-2016-6989.
CVE-2016-6992	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion."
CVE-2016-7020	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-7395	SkPath.cpp in Skia, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, does not properly validate the return values of ChopMonoAtY calls, which allows remote attackers to cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified other impact via crafted graphics data.
CVE-2016-7549	Google Chrome before 53.0.2785.113 does not ensure that the recipient of a certain IPC message is a valid RenderFrame or RenderWidget, which allows remote attackers to cause a denial of service (invalid pointer dereference and application crash) or possibly have unspecified other impact by leveraging access to a renderer process, related to render_frame_host_impl.cc and render_widget_host_impl.cc, as demonstrated by a Password Manager message.
CVE-2016-7855	Use-after-free vulnerability in Adobe Flash Player before 23.0.0.205 on Windows and OS X and before 11.2.202.643 on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in October 2016.
CVE-2016-7857	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7858	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7859	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-

	free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7860	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7861	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7862	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7863	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7864	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7865	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7867	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class related to bookmarking in searches. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7868	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class related to alternation functionality. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7869	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class related to backtrack search functionality. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7870	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class for specific search strategies. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7871	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory

	corruption vulnerability in the Worker class. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7872	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the MovieClip class related to objects at multiple presentation levels. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7873	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulnerability in the PSDK class related to ad policy functionality method. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7874	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulnerability in the NetConnection class when handling the proxy types. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7875	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable integer overflow vulnerability in the BitmapData class. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7876	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulnerability in the Clipboard class related to data handling functionality. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7877	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the Action Message Format serialization (AFM0). Successful exploitation could lead to arbitrary code execution.
CVE-2016-7878	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the PSDK's MediaPlayer class. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7879	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the NetConnection class when handling an attached script object. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7880	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability when setting the length property of an array object. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7881	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after

	free vulnerability in the MovieClip class when handling conversion to an object. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7890	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have security bypass vulnerability in the implementation of the same origin policy.
CVE-2016-7892	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the TextField class. Successful exploitation could lead to arbitrary code execution.
CVE-2016-9650	Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled iframes, which allowed a remote attacker to bypass a no-referrer policy via a crafted HTML page.
CVE-2016-9651	A missing check for whether a property of a JS object is private in V8 in Google Chrome prior to 55.0.2883.75 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2016-9652	Multiple unspecified vulnerabilities in Google Chrome before 55.0.2883.75.
CVE-2017-1000242	Jenkins Git Client Plugin 2.4.2 and earlier creates temporary file with insecure permissions resulting in information disclosure
CVE-2017-11213	An issue was discovered in Adobe Flash Player 27.0.0.183 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer due to an integer overflow; the computation is part of the abstraction that creates an arbitrarily sized transparent or opaque bitmap image. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure.
CVE-2017-11215	An issue was discovered in Adobe Flash Player 27.0.0.183 and earlier versions. This vulnerability is an instance of a use after free vulnerability in the Primetime SDK. The mismatch between an old and a new object can provide an attacker with unintended memory access -- potentially leading to code corruption, control-flow hijack, or an information leak attack. Successful exploitation could lead to arbitrary code execution.
CVE-2017-11225	An issue was discovered in Adobe Flash Player 27.0.0.183 and earlier versions. This vulnerability is an instance of a use after free vulnerability in the Primetime SDK metadata functionality. The mismatch between an old and a new object can provide an attacker with unintended memory access -- potentially

	leading to code corruption, control-flow hijack, or an information leak attack. Successful exploitation could lead to arbitrary code execution.
CVE-2017-11281	Adobe Flash Player has an exploitable memory corruption vulnerability in the text handling function. Successful exploitation could lead to arbitrary code execution. This affects 26.0.0.151 and earlier.
CVE-2017-11282	Adobe Flash Player has an exploitable memory corruption vulnerability in the MP4 atom parser. Successful exploitation could lead to arbitrary code execution. This affects 26.0.0.151 and earlier.
CVE-2017-11292	Adobe Flash Player version 27.0.0.159 and earlier has a flawed bytecode verification procedure, which allows for an untrusted value to be used in the calculation of an array index. This can lead to type confusion, and successful exploitation could lead to arbitrary code execution.
CVE-2017-12635	Due to differences in the Erlang-based JSON parser and JavaScript-based JSON parser, it is possible in Apache CouchDB before 1.7.0 and 2.x before 2.1.1 to submit _users documents with duplicate keys for 'roles' used for access control within the database, including the special case '_admin' role, that denotes administrative users. In combination with CVE-2017-12636 (Remote Code Execution), this can be used to give non-admin users access to arbitrary shell commands on the server as the database system user. The JSON parser differences result in behaviour that if two 'roles' keys are available in the JSON, the second one will be used for authorising the document write, but the first 'roles' key is used for subsequent authorization for the newly created user. By design, users can not assign themselves roles. The vulnerability allows non-admin users to give themselves admin privileges.
CVE-2017-12636	CouchDB administrative users can configure the database server via HTTP(S). Some of the configuration options include paths for operating system-level binaries that are subsequently launched by CouchDB. This allows an admin user in Apache CouchDB before 1.7.0 and 2.x before 2.1.1 to execute arbitrary shell commands as the CouchDB user, including downloading and executing scripts from the public internet.
CVE-2017-15048	Stack-based buffer overflow in the ZoomLauncher binary in the Zoom client for Linux before 2.0.115900.1201 allows remote attackers to execute arbitrary code by leveraging the zoommtg:// scheme handler.
CVE-2017-15049	The ZoomLauncher binary in the Zoom client for Linux before 2.0.115900.1201 does not properly sanitize

	user input when constructing a shell command, which allows remote attackers to execute arbitrary code by leveraging the zoommtg:// scheme handler.
CVE-2017-15386	Incorrect implementation in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-15387	Insufficient enforcement of Content Security Policy in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to open javascript: URL windows when they should not be allowed to via a crafted HTML page.
CVE-2017-15388	Iteration through non-finite points in Skia in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-15389	An insufficient watchdog timer in navigation in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-15390	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-15391	Insufficient Policy Enforcement in Extensions in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to access Extension pages without authorisation via a crafted HTML page.
CVE-2017-15392	Insufficient data validation in V8 in Google Chrome prior to 62.0.3202.62 allowed an attacker who can write to the Windows Registry to potentially exploit heap corruption via a crafted Windows Registry entry, related to PlatformIntegration.
CVE-2017-15393	Insufficient Policy Enforcement in Devtools remote debugging in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to obtain access to remote debugging functionality via a crafted HTML page, aka a Referer leak.
CVE-2017-15394	Insufficient Policy Enforcement in Extensions in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform domain spoofing in permission dialogs via IDN homographs in a crafted Chrome Extension.
CVE-2017-15395	A use after free in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka an ImageCapture NULL pointer dereference.
CVE-2017-15396	A stack buffer overflow in NumberingSystem in International Components for Unicode (ICU) for C/C++ before 60.2, as used in V8 in Google Chrome prior to 62.0.3202.75 and other products, allowed a remote

	attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-15398	A stack buffer overflow in the QUIC networking stack in Google Chrome prior to 62.0.3202.89 allowed a remote attacker to gain code execution via a malicious server.
CVE-2017-15399	A use after free in V8 in Google Chrome prior to 62.0.3202.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-15406	A stack buffer overflow in V8 in Google Chrome prior to 62.0.3202.75 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-15407	Out-of-bounds Write in the QUIC networking stack in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to gain code execution via a malicious server.
CVE-2017-15408	Heap buffer overflow in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file that is mishandled by PDFium.
CVE-2017-15409	Heap buffer overflow in Skia in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-15410	Use after free in PDFium in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-15411	Use after free in PDFium in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-15412	Use after free in libxml2 before 2.9.5, as used in Google Chrome prior to 63.0.3239.84 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-15413	Type confusion in WebAssembly in V8 in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-15415	Incorrect serialization in IPC in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to leak the value of a pointer via a crafted HTML page.
CVE-2017-15416	Heap buffer overflow in Blob API in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka a Blink out-of-bounds read.
CVE-2017-15417	Inappropriate implementation in Skia canvas composite operations in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2017-15418	Use of uninitialized memory in Skia in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to

	obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-15419	Insufficient policy enforcement in Resource Timing API in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to infer browsing history by triggering a leaked cross-origin URL via a crafted HTML page.
CVE-2017-15420	Incorrect handling of back navigations in error pages in Navigation in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-15422	Integer overflow in international date handling in International Components for Unicode (ICU) for C/C++ before 60.1, as used in V8 in Google Chrome prior to 63.0.3239.84 and other products, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-15423	Inappropriate implementation in BoringSSL SPAKE2 in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to leak the low-order bits of SHA512(password) by inspecting protocol traffic.
CVE-2017-15424	Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-15425	Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-15426	Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-15427	Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a socially engineered user to XSS themselves by dragging and dropping a javascript: URL into the URL bar.
CVE-2017-15428	Insufficient data validation in V8 builtins string generator could lead to out of bounds read and write access in V8 in Google Chrome prior to 62.0.3202.94 and allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2017-15429	Inappropriate implementation in V8 WebAssembly JS bindings in Google Chrome prior to 63.0.3239.108 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-15430	Insufficient data validation in Chromecast plugin in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.

CVE-2017-18926	raptor_xml_writer_start_element_common in raptor_xml_writer.c in Raptor RDF Syntax Library 2.0.15 miscalculates the maximum nspace declarations for the XML writer, leading to heap-based buffer overflows (sometimes seen in raptor_qname_format_as_xml).
CVE-2017-2925	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable memory corruption vulnerability in the JPEG XR codec. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2926	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable memory corruption vulnerability related to processing of atoms in MP4 files. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2927	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable heap overflow vulnerability when processing Adobe Texture Format files. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2928	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable memory corruption vulnerability related to setting visual mode effects. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2930	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable memory corruption vulnerability due to a concurrency error when manipulating a display list. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2931	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable memory corruption vulnerability related to the parsing of SWF metadata. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2932	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable use after free vulnerability in the ActionScript MovieClip class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2933	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable heap overflow vulnerability related to texture compression. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2934	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable heap overflow vulnerability when parsing Adobe Texture Format files. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2935	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable heap overflow vulnerability when processing the Flash Video container file format. Successful exploitation could lead to arbitrary code execution.

CVE-2017-2936	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable use after free vulnerability in the ActionScript FileReference class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2937	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable use after free vulnerability in the ActionScript FileReference class, when using class inheritance. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2938	Adobe Flash Player versions 24.0.0.186 and earlier have a security bypass vulnerability related to handling TCP connections.
CVE-2017-2982	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability in a routine related to player shutdown. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2984	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable heap overflow vulnerability in the h264 decoder routine. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2985	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability in the ActionScript 3 BitmapData class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2986	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable heap overflow vulnerability in the Flash Video (FLV) codec. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2987	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable integer overflow vulnerability related to Flash Broker COM. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2988	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability when performing garbage collection. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2990	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability in the h264 decompression routine. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2991	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability in the h264 codec (related to decompression). Successful exploitation could lead to arbitrary code execution.
CVE-2017-2992	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable heap overflow vulnerability when parsing an MP4 header. Successful exploitation could lead to arbitrary code execution.

CVE-2017-2993	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability related to event handlers. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2994	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability in Primetime SDK event dispatch. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2995	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable type confusion vulnerability related to the MessageChannel class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2996	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability in Primetime SDK. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2997	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable buffer overflow / underflow vulnerability in the Primetime TVSDK that supports customizing ad information. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2998	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable memory corruption vulnerability in the Primetime TVSDK API functionality related to timeline interactions. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2999	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable memory corruption vulnerability in the Primetime TVSDK functionality related to hosting playback surface. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3000	Adobe Flash Player versions 24.0.0.221 and earlier have a vulnerability in the random number generator used for constant blinding. Successful exploitation could lead to information disclosure.
CVE-2017-3001	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability related to garbage collection in the ActionScript 2 VM. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3002	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability in the ActionScript2 TextField object related to the variable property. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3003	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability related to an interaction between the privacy user interface and the ActionScript 2 Camera object. Successful exploitation could lead to arbitrary code execution.

CVE-2017-3058	Adobe Flash Player versions 25.0.0.127 and earlier have an exploitable use after free vulnerability in the sound class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3059	Adobe Flash Player versions 25.0.0.127 and earlier have an exploitable use after free vulnerability in the internal script object. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3060	Adobe Flash Player versions 25.0.0.127 and earlier have an exploitable memory corruption vulnerability in the ActionScript2 code parser. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3061	Adobe Flash Player versions 25.0.0.127 and earlier have an exploitable memory corruption vulnerability in the SWF parser. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3062	Adobe Flash Player versions 25.0.0.127 and earlier have an exploitable use after free vulnerability in ActionScript2 when creating a getter/setter property. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3063	Adobe Flash Player versions 25.0.0.127 and earlier have an exploitable use after free vulnerability in the ActionScript2 NetStream class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3064	Adobe Flash Player versions 25.0.0.127 and earlier have an exploitable memory corruption vulnerability when parsing a shape outline. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3068	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable memory corruption vulnerability in the Advanced Video Coding engine. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3069	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable memory corruption vulnerability in the BlendMode class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3070	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable memory corruption vulnerability in the ConvolutionFilter class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3071	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable use after free vulnerability when masking display objects. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3072	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable memory corruption vulnerability in the BitmapData class. Successful exploitation could lead to arbitrary code execution.

CVE-2017-3073	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable use after free vulnerability when handling multiple mask properties of display objects, aka memory corruption. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3074	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable memory corruption vulnerability in the Graphics class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3075	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability when manipulating the ActionsScript 2 XML class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3076	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the MPEG-4 AVC module. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3077	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the PNG image parser. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3078	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the Adobe Texture Format (ATF) module. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3079	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the internal representation of raster data. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3080	Adobe Flash Player versions 26.0.0.131 and earlier have a security bypass vulnerability related to the Flash API used by Internet Explorer. Successful exploitation could lead to information disclosure.
CVE-2017-3081	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability during internal computation caused by multiple display object mask manipulations. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3082	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the LocaleID class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3083	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability in the Primetime SDK functionality related to the profile metadata of the media stream. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3084	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability in

	the advertising metadata functionality. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3085	Adobe Flash Player versions 26.0.0.137 and earlier have a security bypass vulnerability that leads to information disclosure when performing URL redirect.
CVE-2017-3099	Adobe Flash Player versions 26.0.0.131 and earlier have an exploitable memory corruption vulnerability in the Action Script 3 raster data model. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3100	Adobe Flash Player versions 26.0.0.131 and earlier have an exploitable memory corruption vulnerability in the Action Script 2 BitmapData class. Successful exploitation could lead to memory address disclosure.
CVE-2017-3106	Adobe Flash Player versions 26.0.0.137 and earlier have an exploitable type confusion vulnerability when parsing SWF files. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3112	An issue was discovered in Adobe Flash Player 27.0.0.183 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is part of AdobePSDK metadata. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure.
CVE-2017-3114	An issue was discovered in Adobe Flash Player 27.0.0.183 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is part of providing language- and region- or country-specific functionality. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure.
CVE-2017-3248	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Core Components). Supported versions that are affected are 10.3.6.0, 12.1.3.0, 12.2.1.0 and 12.2.1.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS v3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts).
CVE-2017-5006	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled object owner relationships, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.

CVE-2017-5007	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled the sequence of events when closing a page, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-5008	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed attacker controlled JavaScript to be run during the invocation of a private script method, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-5009	WebRTC in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5010	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, resolved promises in an inappropriate context, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-5011	Google Chrome prior to 56.0.2924.76 for Windows insufficiently sanitized DevTools URLs, which allowed a remote attacker who convinced a user to install a malicious extension to read filesystem contents via a crafted HTML page.
CVE-2017-5012	A heap buffer overflow in V8 in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5013	Google Chrome prior to 56.0.2924.76 for Linux incorrectly handled new tab page navigations in non-selected tabs, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-5014	Heap buffer overflow during image processing in Skia in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5015	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled Unicode glyphs, which allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5016	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to prevent certain UI elements from being displayed by

	non-visible pages, which allowed a remote attacker to show certain UI elements on a page they don't control via a crafted HTML page.
CVE-2017-5017	Interactions with the OS in Google Chrome prior to 56.0.2924.76 for Mac insufficiently cleared video memory, which allowed a remote attacker to possibly extract image fragments on systems with GeForce 8600M graphics chips via a crafted HTML page.
CVE-2017-5018	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, had an insufficiently strict content security policy on the Chrome app launcher page, which allowed a remote attacker to inject scripts or HTML into a privileged page via a crafted HTML page.
CVE-2017-5019	A use after free in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5020	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to require a user gesture for powerful download operations, which allowed a remote attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted HTML page.
CVE-2017-5021	A use after free in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5022	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to properly enforce unsafe-inline content security policy, which allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2017-5023	Type confusion in Histogram in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit a near null dereference via a crafted HTML page.
CVE-2017-5024	FFmpeg in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2017-5025	FFmpeg in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted video file.

CVE-2017-5026	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to prevent alerts from being displayed by swapped out frames, which allowed a remote attacker to show alerts on a page they don't control via a crafted HTML page.
CVE-2017-5027	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to properly enforce unsafe-inline content security policy, which allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2017-5029	The xsltAddTextString function in transform.c in libxslt 1.1.29, as used in Blink in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android, lacked a check for integer overflow during a size calculation, which allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2017-5030	Incorrect handling of complex species in V8 in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac and 57.0.2987.108 for Android allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2017-5031	A use after free in ANGLE in Google Chrome prior to 57.0.2987.98 for Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5032	PDFium in Google Chrome prior to 57.0.2987.98 for Windows could be made to increment off the end of a buffer, which allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-5033	Blink in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android failed to correctly propagate CSP restrictions to local scheme pages, which allowed a remote attacker to bypass content security policy via a crafted HTML page, related to the unsafe-inline keyword.
CVE-2017-5034	A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Linux and Windows allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2017-5035	Google Chrome prior to 57.0.2987.98 for Windows and Mac had a race condition, which could cause Chrome to display incorrect certificate information for a site.
CVE-2017-5036	A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to have an unspecified impact via a crafted PDF file.
CVE-2017-5037	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and

	57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5038	Chrome Apps in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac had a use after free bug in GuestView, which allowed a remote attacker to perform an out of bounds memory read via a crafted Chrome extension.
CVE-2017-5039	A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-5040	V8 in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android was missing a neutering check, which allowed a remote attacker to read values in memory via a crafted HTML page.
CVE-2017-5041	Google Chrome prior to 57.0.2987.100 incorrectly handled back-forward navigation, which allowed a remote attacker to display incorrect information for a site via a crafted HTML page.
CVE-2017-5042	Cast in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android sent cookies to sites discovered via SSDP, which allowed an attacker on the local network segment to initiate connections to arbitrary URLs and observe any plaintext cookies sent.
CVE-2017-5043	Chrome Apps in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac had a use after free bug in GuestView, which allowed a remote attacker to perform an out of bounds memory read via a crafted Chrome extension.
CVE-2017-5044	Heap buffer overflow in filter processing in Skia in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5045	XSS Auditor in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed detection of a blocked iframe load, which allowed a remote attacker to brute force JavaScript variables via a crafted HTML page.
CVE-2017-5046	V8 in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android had insufficient policy enforcement, which allowed a remote attacker to spoof the location object via a crafted HTML page, related to Blink information disclosure.
CVE-2017-5047	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and

	57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5048	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5049	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5050	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5051	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5052	An incorrect assumption about block structure in Blink in Google Chrome prior to 57.0.2987.133 for Mac, Windows, and Linux, and 57.0.2987.132 for Android, allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page that triggers improper casting.
CVE-2017-5053	An out-of-bounds read in V8 in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page, related to Array.prototype.indexOf.
CVE-2017-5054	An out-of-bounds read in V8 in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker to obtain heap memory contents via a crafted HTML page.
CVE-2017-5055	A use after free in printing in Google Chrome prior to 57.0.2987.133 for Linux and Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5056	A use after free in Blink in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5057	Type confusion in PDFium in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and

	58.0.3029.83 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2017-5058	A use after free in PrintPreview in Google Chrome prior to 58.0.3029.81 for Windows allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2017-5059	Type confusion in Blink in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac, and 58.0.3029.83 for Android, allowed a remote attacker to potentially obtain code execution via a crafted HTML page.
CVE-2017-5060	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5061	A race condition in navigation in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-5062	A use after free in Chrome Apps in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to potentially perform out of bounds memory access via a crafted Chrome extension.
CVE-2017-5063	A numeric overflow in Skia in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac, and 58.0.3029.83 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5064	Incorrect handling of DOM changes in Blink in Google Chrome prior to 58.0.3029.81 for Windows allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5065	Lack of an appropriate action on page navigation in Blink in Google Chrome prior to 58.0.3029.81 for Windows and Mac allowed a remote attacker to potentially confuse a user into making an incorrect security decision via a crafted HTML page.
CVE-2017-5066	Insufficient consistency checks in signature handling in the networking stack in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to incorrectly accept a badly formed X.509 certificate via a crafted HTML page.
CVE-2017-5067	An insufficient watchdog timer in navigation in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and

	Mac allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-5068	Incorrect handling of picture ID in WebRTC in Google Chrome prior to 58.0.3029.96 for Mac, Windows, and Linux allowed a remote attacker to trigger a race condition via a crafted HTML page.
CVE-2017-5069	Incorrect MIME type of XSS-Protection reports in Blink in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac, and 58.0.3029.83 for Android, allowed a remote attacker to circumvent Cross-Origin Resource Sharing checks via a crafted HTML page.
CVE-2017-5070	Type confusion in V8 in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2017-5071	Insufficient validation of untrusted input in V8 in Google Chrome prior to 59.0.3071.86 for Linux, Windows and Mac, and 59.0.3071.92 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5072	Inappropriate implementation in Omnibox in Google Chrome prior to 59.0.3071.92 for Android allowed a remote attacker to perform domain spoofing with RTL characters via a crafted URL page.
CVE-2017-5073	Use after free in print preview in Blink in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5074	A use after free in Chrome Apps in Google Chrome prior to 59.0.3071.86 for Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page, related to Bluetooth.
CVE-2017-5075	Inappropriate implementation in CSP reporting in Blink in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to obtain the value of url fragments via a crafted HTML page.
CVE-2017-5076	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5077	Insufficient validation of untrusted input in Skia in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.

CVE-2017-5078	Insufficient validation of untrusted input in Blink's mailto: handling in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac allowed a remote attacker to perform command injection via a crafted HTML page, a similar issue to CVE-2004-0121. For example, characters such as * have an incorrect interaction with xdg-email in xdg-utils, and a space character can be used in front of a command-line argument.
CVE-2017-5079	Inappropriate implementation in Blink in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed a remote attacker to display UI on a non attacker controlled tab via a crafted HTML page.
CVE-2017-5080	A use after free in credit card autofill in Google Chrome prior to 59.0.3071.86 for Linux and Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5081	Lack of verification of an extension's locale folder in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed an attacker with local write access to modify extensions by modifying extension files.
CVE-2017-5082	Failure to take advantage of available mitigations in credit card autofill in Google Chrome prior to 59.0.3071.92 for Android allowed a local attacker to take screen shots of credit card information via a crafted HTML page.
CVE-2017-5083	Inappropriate implementation in Blink in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed a remote attacker to display UI on a non attacker controlled tab via a crafted HTML page.
CVE-2017-5085	Inappropriate implementation in Bookmarks in Google Chrome prior to 59 for iOS allowed a remote attacker who convinced the user to perform certain operations to run JavaScript on chrome:// pages via a crafted bookmark.
CVE-2017-5086	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 59.0.3071.86 for Windows and Mac allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5087	A use after free in Blink in Google Chrome prior to 59.0.3071.104 for Mac, Windows, and Linux, and 59.0.3071.117 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page, aka an IndexedDB sandbox escape.
CVE-2017-5088	Insufficient validation of untrusted input in V8 in Google Chrome prior to 59.0.3071.104 for Mac, Windows, and Linux, and 59.0.3071.117 for Android, allowed a remote

	attacker to perform out of bounds memory access via a crafted HTML page.
CVE-2017-5089	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 59.0.3071.104 for Mac allowed a remote attacker to perform domain spoofing via a crafted domain name.
CVE-2017-5091	A use after free in IndexedDB in Google Chrome prior to 60.0.3112.78 for Linux, Android, Windows, and Mac allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5092	Insufficient validation of untrusted input in PPAPI Plugins in Google Chrome prior to 60.0.3112.78 for Windows allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2017-5093	Inappropriate implementation in modal dialog handling in Blink in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to prevent a full screen warning from being displayed via a crafted HTML page.
CVE-2017-5094	Type confusion in extensions JavaScript bindings in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to potentially maliciously modify objects via a crafted HTML page.
CVE-2017-5095	Stack overflow in PDFium in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to potentially exploit stack corruption via a crafted PDF file.
CVE-2017-5097	Insufficient validation of untrusted input in Skia in Google Chrome prior to 60.0.3112.78 for Linux allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5098	A use after free in V8 in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5099	Insufficient validation of untrusted input in PPAPI Plugins in Google Chrome prior to 60.0.3112.78 for Mac allowed a remote attacker to potentially gain privilege elevation via a crafted HTML page.
CVE-2017-5100	A use after free in Apps in Google Chrome prior to 60.0.3112.78 for Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5101	Inappropriate implementation in Omnibox in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to spoof the contents of the Omnibox via a crafted HTML page.

CVE-2017-5102	Use of an uninitialized value in Skia in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5103	Use of an uninitialized value in Skia in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5104	Inappropriate implementation in interstitials in Google Chrome prior to 60.0.3112.78 for Mac allowed a remote attacker to spoof the contents of the omnibox via a crafted HTML page.
CVE-2017-5105	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5106	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5107	A timing attack in SVG rendering in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to extract pixel values from a cross-origin page being iframe'd via a crafted HTML page.
CVE-2017-5108	Type confusion in PDFium in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to potentially maliciously modify objects via a crafted PDF file.
CVE-2017-5109	Inappropriate implementation of unload handler handling in permission prompts in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to display UI on a non attacker controlled tab via a crafted HTML page.
CVE-2017-5110	Inappropriate implementation of the web payments API on blob: and data: schemes in Web Payments in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to spoof the contents of the Omnibox via a crafted HTML page.
CVE-2017-5111	A use after free in PDFium in Google Chrome prior to 61.0.3163.79 for Linux, Windows, and Mac allowed a remote attacker to potentially exploit memory corruption via a crafted PDF file.

CVE-2017-5112	Heap buffer overflow in WebGL in Google Chrome prior to 61.0.3163.79 for Windows allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2017-5113	Math overflow in Skia in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5114	Inappropriate use of partition alloc in PDFium in Google Chrome prior to 61.0.3163.79 for Linux, Windows, and Mac, and 61.0.3163.81 for Android, allowed a remote attacker to potentially exploit memory corruption via a crafted PDF file.
CVE-2017-5115	Type confusion in V8 in Google Chrome prior to 61.0.3163.79 for Windows allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2017-5116	Type confusion in V8 in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2017-5117	Use of an uninitialized value in Skia in Google Chrome prior to 61.0.3163.79 for Linux and Windows allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5118	Blink in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, failed to correctly propagate CSP restrictions to javascript scheme pages, which allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2017-5119	Use of an uninitialized value in Skia in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5120	Inappropriate use of www mismatch redirects in browser navigation in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to potentially downgrade HTTPS requests to HTTP via a crafted HTML page. In other words, Chrome could transmit cleartext even though the user had entered an https URL, because of a misdesigned workaround for cases where the domain name in a URL almost matches the domain name in an X.509 server certificate (but differs in the initial "www." substring).

CVE-2017-5121	Inappropriate use of JIT optimisation in V8 in Google Chrome prior to 61.0.3163.100 for Linux, Windows, and Mac allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page, related to the escape analysis phase.
CVE-2017-5122	Inappropriate use of table size handling in V8 in Google Chrome prior to 61.0.3163.100 for Windows allowed a remote attacker to trigger out-of-bounds access via a crafted HTML page.
CVE-2017-5124	Incorrect application of sandboxing in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted MHTML page.
CVE-2017-5125	Heap buffer overflow in Skia in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5126	A use after free in PDFium in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-5127	Use after free in PDFium in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-5128	Heap buffer overflow in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, related to WebGL.
CVE-2017-5129	A use after free in WebAudio in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5130	An integer overflow in xmlmemory.c in libxml2 before 2.9.5, as used in Google Chrome prior to 62.0.3202.62 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted XML file.
CVE-2017-5131	An integer overflow in Skia in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka an out-of-bounds write.
CVE-2017-5132	Inappropriate implementation in V8 in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka incorrect WebAssembly stack manipulation.
CVE-2017-5133	Off-by-one read/write on the heap in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to corrupt memory and possibly leak information and potentially execute code via a crafted PDF file.
CVE-2017-7000	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. The issue involves the "SQLite" component.

	It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-9111	In OpenEXR 2.2.0, an invalid write of size 8 in the storeSSE function in ImfOptimizedPixelReading.h could cause the application to crash or execute arbitrary code.
CVE-2017-9113	In OpenEXR 2.2.0, an invalid write of size 1 in the bufferedReadPixels function in ImfInputFile.cpp could cause the application to crash or execute arbitrary code.
CVE-2017-9115	In OpenEXR 2.2.0, an invalid write of size 2 in the = operator function in half.h could cause the application to crash or execute arbitrary code.
CVE-2018-1000500	Busybox contains a Missing SSL certificate validation vulnerability in The "busybox wget" applet that can result in arbitrary code execution. This attack appear to be exploitable via Simply download any file over HTTPS using "busybox wget https://compromised-domain.com/important-file".
CVE-2018-1000852	FreeRDP FreeRDP 2.0.0-rc3 released version before commit 205c612820dac644d665b5bb1cdf437dc5ca01e3 contains a Other/Unknown vulnerability in channels/drdynvc/client/drdynvc_main.c, drdynvc_process_capability_request that can result in The RDP server can read the client's memory.. This attack appear to be exploitable via RDPClient must connect the rdp server with echo option. This vulnerability appears to have been fixed in after commit 205c612820dac644d665b5bb1cdf437dc5ca01e3.
CVE-2018-1000861	A code execution vulnerability exists in the Stapler web framework used by Jenkins 2.153 and earlier, LTS 2.138.3 and earlier in stapler/core/src/main/java/org/kohsuke/stapler/MetaClass.java that allows attackers to invoke some methods on Java objects by accessing crafted URLs that were not intended to be invoked this way.
CVE-2018-1002105	In all Kubernetes versions prior to v1.10.11, v1.11.5, and v1.12.3, incorrect handling of error responses to proxied upgrade requests in the kube-apiserver allowed specially crafted requests to establish a connection through the Kubernetes API server to backend servers, then send arbitrary requests over the same connection directly to the backend, authenticated with the Kubernetes API server's TLS credentials used to establish the backend connection.
CVE-2018-10237	Unbounded memory allocation in Google Guava 11.0 through 24.x before 24.1.1 allows remote attackers to conduct denial of service attacks against servers

	that depend on this library and deserialize attacker-provided data, because the AtomicDoubleArray class (when serialized with Java serialization) and the CompoundOrdering class (when serialized with GWT serialization) perform eager allocation without appropriate checks on what a client has sent and whether the data size is reasonable.
CVE-2018-11212	An issue was discovered in libjpeg 9a and 9d. The alloc_sarray function in jmemmgr.c allows remote attackers to cause a denial of service (divide-by-zero error) via a crafted file.
CVE-2018-1128	It was found that cephx authentication protocol did not verify ceph clients correctly and was vulnerable to replay attack. Any attacker having access to ceph cluster network who is able to sniff packets on network can use this vulnerability to authenticate with ceph service and perform actions allowed by ceph service. Ceph branches master, mimic, luminous and jewel are believed to be vulnerable.
CVE-2018-11769	CouchDB administrative users before 2.2.0 can configure the database server via HTTP(S). Due to insufficient validation of administrator-supplied configuration settings via the HTTP API, it is possible for a CouchDB administrator user to escalate their privileges to that of the operating system's user under which CouchDB runs, by bypassing the blacklist of configuration settings that are not allowed to be modified via the HTTP API. This privilege escalation effectively allows a CouchDB admin user to gain arbitrary remote code execution, bypassing CVE-2017-12636 and CVE-2018-8007.
CVE-2018-12824	Adobe Flash Player 30.0.0.134 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-12825	Adobe Flash Player 30.0.0.134 and earlier have a security bypass vulnerability. Successful exploitation could lead to security mitigation bypass.
CVE-2018-12826	Adobe Flash Player 30.0.0.134 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-12827	Adobe Flash Player 30.0.0.134 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-12828	Adobe Flash Player 30.0.0.134 and earlier have a "use of a component with a known vulnerability" vulnerability. Successful exploitation could lead to privilege escalation.
CVE-2018-1285	Apache log4net versions before 2.0.10 do not disable XML external entities when parsing log4net configuration files. This allows for XXE-based attacks

	in applications that accept attacker-controlled log4net configuration files.
CVE-2018-15715	Zoom clients on Windows (before version 4.1.34814.1119), Mac OS (before version 4.1.34801.1116), and Linux (2.4.129780.0915 and below) are vulnerable to unauthorized message processing. A remote unauthenticated attacker can spoof UDP messages from a meeting attendee or Zoom server in order to invoke functionality in the target client. This allows the attacker to remove attendees from meetings, spoof messages from users, or hijack shared screens.
CVE-2018-15967	Adobe Flash Player versions 30.0.0.154 and earlier have a privilege escalation vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-15978	Flash Player versions 31.0.0.122 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-15981	Flash Player versions 31.0.0.148 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2018-15982	Flash Player versions 31.0.0.153 and earlier, and 31.0.0.108 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2018-15983	Flash Player versions 31.0.0.153 and earlier, and 31.0.0.108 and earlier have an insecure library loading (dll hijacking) vulnerability. Successful exploitation could lead to privilege escalation.
CVE-2018-16065	A Javascript reentrancy issues that caused a use-after-free in V8 in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-16066	A use after free in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-16067	A use after free in WebAudio in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-16068	Missing validation in Mojo in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2018-16069	Unintended floating-point error accumulation in SwiftShader in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-16070	Integer overflows in Skia in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2018-16071	A use after free in WebRTC in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2018-16073	Insufficient policy enforcement in site isolation in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2018-16074	Insufficient policy enforcement in site isolation in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2018-16075	Insufficient file type enforcement in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to obtain local file data via a crafted HTML page.
CVE-2018-16076	Missing bounds check in PDFium in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2018-16077	Object lifecycle issue in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2018-16078	Unsafe handling of credit card details in Autofill in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2018-16079	A race condition between permission prompts and navigations in Prompts in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-16080	A missing check for popup window handling in Fullscreen in Google Chrome on macOS prior to 69.0.3497.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-16081	Allowing the chrome.debugger API to run on file:// URLs in DevTools in Google Chrome prior to 69.0.3497.81 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system without file access permission via a crafted Chrome Extension.
CVE-2018-16082	An out of bounds read in Swiftshader in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2018-16083	An out of bounds read in forward error correction code in WebRTC in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.

CVE-2018-16084	The default selected dialog button in CustomHandlers in Google Chrome prior to 69.0.3497.81 allowed a remote attacker who convinced the user to perform certain operations to open external programs via a crafted HTML page.
CVE-2018-16085	A use after free in ResourceCoordinator in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-17462	Incorrect refcounting in AppCache in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to perform a sandbox escape via a crafted HTML page.
CVE-2018-17463	Incorrect side effect annotation in V8 in Google Chrome prior to 70.0.3538.64 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-17464	Incorrect handling of history on iOS in Navigation in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-17465	Incorrect implementation of object trimming in V8 in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2018-17466	Incorrect texture handling in Angle in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-17467	Insufficiently quick clearing of stale rendered content in Navigation in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-17468	Incorrect handling of timer information during navigation in Blink in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to obtain cross origin URLs via a crafted HTML page.
CVE-2018-17469	Incorrect handling of PDF filter chains in PDFium in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2018-17470	A heap buffer overflow in GPU in Google Chrome prior to 70.0.3538.67 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2018-17471	Incorrect dialog placement in WebContents in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to obscure the full screen warning via a crafted HTML page.

CVE-2018-17473	Incorrect handling of confusable characters in Omnibox in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-17474	Use after free in HTMLImportsController in Blink in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-17475	Incorrect handling of history on iOS in Navigation in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-17476	Incorrect dialog placement in Cast UI in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to obscure the full screen warning via a crafted HTML page.
CVE-2018-17477	Incorrect dialog placement in Extensions in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of extension popups via a crafted HTML page.
CVE-2018-17478	Incorrect array position calculations in V8 in Google Chrome prior to 70.0.3538.102 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2018-17479	Incorrect object lifetime calculations in GPU code in Google Chrome prior to 70.0.3538.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-17480	Execution of user supplied Javascript during array deserialization leading to an out of bounds write in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-17481	Incorrect object lifecycle handling in PDFium in Google Chrome prior to 71.0.3578.98 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2018-18335	Heap buffer overflow in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18336	Incorrect object lifecycle in PDFium in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2018-18337	Incorrect handling of stylesheets leading to a use after free in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18338	Incorrect, thread-unsafe use of SkImage in Canvas in Google Chrome prior to 71.0.3578.80 allowed a remote

	attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18339	Incorrect object lifecycle in WebAudio in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18340	Incorrect object lifecycle in MediaRecorder in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18341	An integer overflow leading to a heap buffer overflow in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18342	Execution of user supplied Javascript during object deserialization can update object length leading to an out of bounds write in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-18343	Incorrect handing of paths leading to a use after free in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18344	Inappropriate allowance of the setDownloadBehavior devtools protocol feature in Extensions in Google Chrome prior to 71.0.3578.80 allowed a remote attacker with control of an installed extension to access files on the local file system via a crafted Chrome Extension.
CVE-2018-18345	Incorrect handling of blob URLS in Site Isolation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker who had compromised the renderer process to bypass site isolation protections via a crafted HTML page.
CVE-2018-18346	Incorrect handling of alert box display in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to present confusing browser UI via a crafted HTML page.
CVE-2018-18347	Incorrect handling of failed navigations with invalid URLs in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to trick a user into executing javascript in an arbitrary origin via a crafted HTML page.
CVE-2018-18348	Incorrect handling of bidirectional domain names with RTL characters in Omnibox in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.

CVE-2018-18349	Remote frame navigations was incorrectly permitted to local resources in Blink in Google Chrome prior to 71.0.3578.80 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system via a crafted Chrome Extension.
CVE-2018-18350	Incorrect handling of CSP enforcement during navigations in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2018-18351	Lack of proper validation of ancestor frames site when sending lax cookies in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to bypass SameSite cookie policy via a crafted HTML page.
CVE-2018-18352	Service works could inappropriately gain access to cross origin audio in Media in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to bypass same origin policy for audio content via a crafted HTML page.
CVE-2018-18353	Failure to dismiss http auth dialogs on navigation in Network Authentication in Google Chrome on Android prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of an auto dialog via a crafted HTML page.
CVE-2018-18354	Insufficient validate of external protocols in Shell Integration in Google Chrome on Windows prior to 71.0.3578.80 allowed a remote attacker to launch external programs via a crafted HTML page.
CVE-2018-18355	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-18356	An integer overflow in path handling lead to a use after free in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18357	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-18358	Lack of special casing of localhost in WPAD files in Google Chrome prior to 71.0.3578.80 allowed an attacker on the local network segment to proxy resources on localhost via a crafted WPAD file.
CVE-2018-18359	Incorrect handling of Reflect.construct in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.

CVE-2018-18444	makeMultiView.cpp in exrmultiview in OpenEXR 2.3.0 has an out-of-bounds write, leading to an assertion failure or possibly unspecified other impact.
CVE-2018-1922	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is affected by buffer overflow vulnerability that can potentially result in arbitrary code execution. IBM X-Force ID: 152858.
CVE-2018-1923	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is affected by buffer overflow vulnerability that can potentially result in arbitrary code execution. IBM X-Force ID: 152859.
CVE-2018-1978	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-ForceID: 154069.
CVE-2018-1980	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-ForceID: 154078.
CVE-2018-20030	An error when processing the EXIF_IFD_INTEROPERABILITY and EXIF_IFD_EXIF tags within libexif version 0.6.21 can be exploited to exhaust available CPU resources.
CVE-2018-20226	An organization administrator can add a super administrator in THEHIVE PROJECT Cortex before 2.1.3 due to the lack of overriding the Role.toString method.
CVE-2018-2628	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0, 12.1.3.0, 12.2.1.2 and 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2018-2765	Vulnerability in the Oracle Security Service component of Oracle Fusion Middleware (subcomponent: Oracle SSL API). Supported versions that are affected are 11.1.1.9.0, 12.1.3.0.0, 12.2.1.2.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Security Service. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Security Service accessible data. CVSS 3.0 Base Score 7.5

	(Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2018-3191	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0, 12.1.3.0 and 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2018-3822	X-Pack Security versions 6.2.0, 6.2.1, and 6.2.2 are vulnerable to a user impersonation attack via incorrect XML canonicalization and DOM traversal. An attacker might have been able to impersonate a legitimate user if the SAML Identity Provider allows for self registration with arbitrary identifiers and the attacker can register an account which an identifier that shares a suffix with a legitimate account. Both of those conditions must be true in order to exploit this flaw.
CVE-2018-4117	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. watchOS before 4.3 is affected. The issue involves the fetch API in the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.
CVE-2018-4871	An Out-of-bounds Read issue was discovered in Adobe Flash Player before 28.0.0.137. This vulnerability occurs because of computation that reads data that is past the end of the target buffer. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure.
CVE-2018-4877	A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to a dangling pointer in the Primetime SDK related to media player's quality of service functionality. A successful attack can lead to arbitrary code execution.
CVE-2018-4878	A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to a dangling pointer in the Primetime SDK related to media player handling of listener objects. A successful attack can lead to arbitrary code execution. This was exploited in the wild in January and February 2018.

CVE-2018-4919	Adobe Flash Player versions 28.0.0.161 and earlier have an exploitable use after free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-4920	Adobe Flash Player versions 28.0.0.161 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-4932	Adobe Flash Player versions 29.0.0.113 and earlier have an exploitable Use-After-Free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-4933	Adobe Flash Player versions 29.0.0.113 and earlier have an exploitable out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-4934	Adobe Flash Player versions 29.0.0.113 and earlier have an exploitable out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-4935	Adobe Flash Player versions 29.0.0.113 and earlier have an exploitable out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-4936	Adobe Flash Player versions 29.0.0.113 and earlier have an exploitable Heap Overflow vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-4937	Adobe Flash Player versions 29.0.0.113 and earlier have an exploitable out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-4944	Adobe Flash Player versions 29.0.0.140 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-4945	Adobe Flash Player versions 29.0.0.171 and earlier have a Type Confusion vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-5000	Adobe Flash Player versions 29.0.0.171 and earlier have an Integer Overflow vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-5001	Adobe Flash Player versions 29.0.0.171 and earlier have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-5002	Adobe Flash Player versions 29.0.0.171 and earlier have a Stack-based buffer overflow vulnerability.

	Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-5007	Adobe Flash Player 30.0.0.113 and earlier versions have a Type Confusion vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-5008	Adobe Flash Player 30.0.0.113 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-5179	A service worker can send the activate event on itself periodically which allows it to run perpetually, allowing it to monitor activity by users. Affects all versions prior to Firefox 60.
CVE-2018-6031	Use after free in PDFium in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2018-6032	Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user cross-origin data via a crafted HTML page.
CVE-2018-6033	Insufficient data validation in Downloads in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially run arbitrary code outside sandbox via a crafted Chrome Extension.
CVE-2018-6034	Insufficient data validation in WebGL in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6035	Insufficient policy enforcement in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user local file data via a crafted Chrome Extension.
CVE-2018-6036	Insufficient data validation in V8 in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user data via a crafted HTML page.
CVE-2018-6037	Inappropriate implementation in autofill in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to obtain autofill data with insufficient user gestures via a crafted HTML page.
CVE-2018-6038	Heap buffer overflow in WebGL in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6039	Insufficient data validation in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user cross-origin data via a crafted Chrome Extension.

CVE-2018-6040	Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially bypass content security policy via a crafted HTML page.
CVE-2018-6041	Incorrect security UI in navigation in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6042	Incorrect security UI in Omnibox in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6043	Insufficient data validation in External Protocol Handler in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially execute arbitrary programs on user machine via a crafted HTML page.
CVE-2018-6044	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6045	Insufficient policy enforcement in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user local file data via a crafted Chrome Extension.
CVE-2018-6046	Insufficient data validation in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user cross-origin data via a crafted Chrome Extension.
CVE-2018-6047	Insufficient policy enforcement in WebGL in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user redirect URL via a crafted HTML page.
CVE-2018-6048	Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak referrer information via a crafted HTML page.
CVE-2018-6049	Incorrect security UI in permissions prompt in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the origin to which permission is granted via a crafted HTML page.
CVE-2018-6050	Incorrect security UI in Omnibox in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6051	XSS Auditor in Google Chrome prior to 64.0.3282.119, did not ensure the reporting URL was in the same origin as the page it was on, which allowed a remote attacker to obtain referrer details via a crafted HTML page.

CVE-2018-6052	Lack of support for a non standard no-referrer policy value in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to obtain referrer details from a web page that had thought it had opted out of sending referrer data.
CVE-2018-6053	Inappropriate implementation in New Tab Page in Google Chrome prior to 64.0.3282.119 allowed a local attacker to view website thumbnail images after clearing browser data via a crafted HTML page.
CVE-2018-6054	Use after free in WebUI in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2018-6055	Insufficient policy enforcement in Catalog Service in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially run arbitrary code outside sandbox via a crafted HTML page.
CVE-2018-6056	Type confusion could lead to a heap out-of-bounds write in V8 in Google Chrome prior to 64.0.3282.168 allowing a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-6057	Lack of special casing of Android ashmem in Google Chrome prior to 65.0.3325.146 allowed a remote attacker who had compromised the renderer process to bypass inter-process read only guarantees via a crafted HTML page.
CVE-2018-6058	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6059	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6060	Use after free in WebAudio in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6061	A race in the handling of SharedArrayBuffers in WebAssembly in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6062	Heap overflow write in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6063	Incorrect use of mojo::WrapSharedMemoryHandle in Mojo in Google Chrome prior to 65.0.3325.146 allowed a remote attacker who had compromised the renderer

	process to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6064	Type Confusion in the implementation of __defineGetter__ in V8 in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6065	Integer overflow in computing the required allocation size when instantiating a new javascript object in V8 in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6066	Lack of CORS checking by ResourceFetcher/ResourceLoader in Blink in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6067	Incorrect IPC serialization in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6068	Object lifecycle issue in Chrome Custom Tab in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6069	Stack buffer overflow in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6070	Lack of CSP enforcement on WebUI pages in Bink in Google Chrome prior to 65.0.3325.146 allowed an attacker who convinced a user to install a malicious extension to bypass content security policy via a crafted Chrome Extension.
CVE-2018-6071	An integer overflow in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6072	An integer overflow leading to use after free in PDFium in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2018-6073	A heap buffer overflow in WebGL in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6074	Failure to apply Mark-of-the-Web in Downloads in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to bypass OS level controls via a crafted HTML page.
CVE-2018-6075	Incorrect handling of specified filenames in file downloads in Google Chrome prior to 65.0.3325.146

	allowed a remote attacker to leak cross-origin data via a crafted HTML page and user interaction.
CVE-2018-6076	Insufficient encoding of URL fragment identifiers in Blink in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform a DOM based XSS attack via a crafted HTML page.
CVE-2018-6077	Displacement map filters being applied to cross-origin images in Blink SVG rendering in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6078	Incorrect handling of confusable characters in Omnibox in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-6079	Inappropriate sharing of TEXTURE_2D_ARRAY/ TEXTURE_3D data between tabs in WebGL in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6080	Lack of access control checks in Instrumentation in Google Chrome prior to 65.0.3325.146 allowed a remote attacker who had compromised the renderer process to obtain memory metadata from privileged processes .
CVE-2018-6081	XSS vulnerabilities in Interstitials in Google Chrome prior to 65.0.3325.146 allowed an attacker who convinced a user to install a malicious extension or open Developer Console to inject arbitrary scripts or HTML via a crafted HTML page.
CVE-2018-6082	Including port 22 in the list of allowed FTP ports in Networking in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially enumerate internal host services via a crafted HTML page.
CVE-2018-6083	Failure to disallow PWA installation from CSP sandboxed pages in AppManifest in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to access privileged APIs via a crafted HTML page.
CVE-2018-6085	Re-entry of a destructor in Networking Disk Cache in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2018-6086	A double-eviction in the Incognito mode cache that lead to a user-after-free in Networking Disk Cache in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2018-6087	A use-after-free in WebAssembly in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to

	execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-6088	An iterator-invalidation bug in PDFium in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.
CVE-2018-6089	A lack of CORS checks, after a Service Worker redirected to a cross-origin PDF, in Service Worker in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak limited cross-origin data via a crafted HTML page.
CVE-2018-6090	An integer overflow that lead to a heap buffer-overflow in Skia in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-6091	Service Workers can intercept any request made by an <embed> or <object> tag in Fetch API in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6092	An integer overflow on 32-bit systems in WebAssembly in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-6093	Insufficient origin checks in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6094	Inline metadata in GarbageCollection in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6095	Inappropriate dismissal of file picker on keyboard events in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to read local files via a crafted HTML page.
CVE-2018-6096	A JavaScript focused window could overlap the fullscreen notification in Fullscreen in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to obscure the full screen warning via a crafted HTML page.
CVE-2018-6097	Incorrect handling of asynchronous methods in Fullscreen in Google Chrome on macOS prior to 66.0.3359.117 allowed a remote attacker to enter full screen without showing a warning via a crafted HTML page.
CVE-2018-6098	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.

CVE-2018-6099	A lack of CORS checks in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak limited cross-origin data via a crafted HTML page.
CVE-2018-6100	Incorrect handling of confusable characters in URL Formatter in Google Chrome on macOS prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6101	A lack of host validation in DevTools in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code via a crafted HTML page, if the user is running a remote DevTools debugging server.
CVE-2018-6102	Missing confusable characters in Internationalization in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-6103	A stagnant permission prompt in Prompts in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to bypass permission policy via a crafted HTML page.
CVE-2018-6104	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6105	Incorrect handling of confusable characters in Omnibox in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6106	An asynchronous generator may return an incorrect state in V8 in Google Chrome prior to 66.0.3359.117 allowing a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2018-6107	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6108	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted HTML page.
CVE-2018-6109	readAsText() can indefinitely read the file picked by the user, rather than only once at the time the file is picked in File API in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to access data on the user file system without explicit consent via a crafted HTML page.
CVE-2018-6110	Parsing documents as HTML in Downloads in Google Chrome prior to 66.0.3359.117 allowed a remote

	attacker to cause Chrome to execute scripts via a local non-HTML page.
CVE-2018-6111	An object lifetime issue in the developer tools network handler in Google Chrome prior to 66.0.3359.117 allowed a local attacker to execute arbitrary code via a crafted HTML page.
CVE-2018-6112	Making URLs clickable and allowing them to be styled in DevTools in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2018-6113	Improper handling of pending navigation entries in Navigation in Google Chrome on iOS prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2018-6114	Incorrect enforcement of CSP for <object> tags in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2018-6115	Inappropriate setting of the SEE_MASK_FLAG_NO_UI flag in file downloads in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to potentially bypass OS malware checks via a crafted HTML page.
CVE-2018-6116	A nullptr dereference in WebAssembly in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2018-6117	Confusing settings in Autofill in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2018-6119	Incorrect security UI in Omnibox in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6120	An integer overflow that could lead to an attacker-controlled heap out-of-bounds write in PDFium in Google Chrome prior to 66.0.3359.170 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.
CVE-2018-6121	Insufficient validation of input in Blink in Google Chrome prior to 66.0.3359.170 allowed a remote attacker to perform privilege escalation via a crafted HTML page.
CVE-2018-6122	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2018-6123	A use after free in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6124	Type confusion in ReadableStreams in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2018-6125	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6126	A precision error in Skia in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6127	Early free of object in use in IndexDB in Google Chrome prior to 67.0.3396.62 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2018-6128	Incorrect URL parsing in WebKit in Google Chrome on iOS prior to 67.0.3396.62 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2018-6129	Out of bounds array access in WebRTC in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2018-6130	Incorrect handling of object lifetimes in WebRTC in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2018-6131	Object lifecycle issue in WebAssembly in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6132	Uninitialized data in WebRTC in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted video file.
CVE-2018-6133	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6134	Information leak in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to bypass no-referrer policy via a crafted HTML page.
CVE-2018-6135	Lack of clearing the previous site before loading alerts from a new one in Blink in Google Chrome prior to

	67.0.3396.62 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2018-6136	Missing type check in V8 in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6137	CSS Paint API in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6138	Insufficient policy enforcement in Extensions API in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.
CVE-2018-6139	Insufficient target checks on the chrome.debugger API in DevTools in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.
CVE-2018-6140	Allowing the chrome.debugger API to attach to Web UI pages in DevTools in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.
CVE-2018-6141	Insufficient validation of an image filter in Skia in Google Chrome prior to 67.0.3396.62 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6142	Array bounds check failure in V8 in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2018-6143	Insufficient validation in V8 in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6144	Off-by-one error in PDFium in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory write via a crafted PDF file.
CVE-2018-6145	Insufficient data validation in HTML parser in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to bypass same origin policy via a crafted HTML page.
CVE-2018-6147	Lack of secure text entry mode in Browser UI in Google Chrome on Mac prior to 67.0.3396.62 allowed a local attacker to obtain potentially sensitive information from process memory via a local process.
CVE-2018-6148	Incorrect implementation in Content Security Policy in Google Chrome prior to 67.0.3396.79 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.

CVE-2018-6149	Type confusion in JavaScript in Google Chrome prior to 67.0.3396.87 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6150	Incorrect handling of CORS in ServiceWorker in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6151	Bad cast in DevTools in Google Chrome on Win, Linux, Mac, Chrome OS prior to 66.0.3359.117 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted Chrome Extension.
CVE-2018-6152	The implementation of the Page.downloadBehavior backend unconditionally marked downloaded files as safe, regardless of file type in Google Chrome prior to 66.0.3359.117 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted HTML page and user interaction.
CVE-2018-6153	A precision error in Skia in Google Chrome prior to 68.0.3440.75 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6154	Insufficient data validation in WebGL in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6155	Incorrect handling of frames in the VP8 parser in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2018-6156	Incorect derivation of a packet length in WebRTC in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2018-6157	Type confusion in WebRTC in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2018-6158	A race condition in Oilpan in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6159	Insufficient policy enforcement in ServiceWorker in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2018-6161	Insufficient policy enforcement in Blink in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to bypass same origin policy via a crafted HTML page.

CVE-2018-6162	Improper deserialization in WebGL in Google Chrome on Mac prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6163	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6164	Insufficient origin checks for CSS content in Blink in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6165	Incorrect handling of reloads in Navigation in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6166	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6167	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6168	Information leak in media engine in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2018-6169	Lack of timeout on extension install prompt in Extensions in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to trigger installation of an unwanted extension via a crafted HTML page.
CVE-2018-6170	A bad cast in PDFium in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2018-6171	Use after free in Bluetooth in Google Chrome prior to 68.0.3440.75 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory via a crafted Chrome Extension.
CVE-2018-6172	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6173	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.

CVE-2018-6174	Integer overflows in Swiftshader in Google Chrome prior to 68.0.3440.75 potentially allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2018-6175	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6176	Insufficient file type enforcement in Extensions API in Google Chrome prior to 68.0.3440.75 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted Chrome Extension.
CVE-2018-6177	Information leak in media engine in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6178	Eliding from the wrong side in an infobar in DevTools in Google Chrome prior to 68.0.3440.75 allowed an attacker who convinced a user to install a malicious extension to Hide Chrome Security UI via a crafted Chrome Extension.
CVE-2018-6179	Insufficient enforcement of file access permission in the activeTab case in Extensions in Google Chrome prior to 68.0.3440.75 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system via a crafted Chrome Extension.
CVE-2018-7225	An issue was discovered in LibVNCServer through 0.9.11. rfbProcessClientNormalMessage() in rfbserver.c does not sanitize msg.cct.length, leading to access to uninitialized and potentially sensitive data or possibly unspecified other impact (e.g., an integer overflow) via specially crafted VNC packets.
CVE-2018-8007	Apache CouchDB administrative users can configure the database server via HTTP(S). Due to insufficient validation of administrator-supplied configuration settings via the HTTP API, it is possible for a CouchDB administrator user to escalate their privileges to that of the operating system's user that CouchDB runs under, by bypassing the blacklist of configuration settings that are not allowed to be modified via the HTTP API. This privilege escalation effectively allows an existing CouchDB admin user to gain arbitrary remote code execution, bypassing already disclosed CVE-2017-12636. Mitigation: All users should upgrade to CouchDB releases 1.7.2 or 2.1.2.
CVE-2019-1003003	An improper authorization vulnerability exists in Jenkins 2.158 and earlier, LTS 2.150.1 and earlier in core/src/main/java/hudson/security/TokenBasedRememberMeServices2.java that allows attackers with Overall/RunScripts permission

	to craft Remember Me cookies that would never expire, allowing e.g. to persist access to temporarily compromised user accounts.
CVE-2019-1003004	An improper authorization vulnerability exists in Jenkins 2.158 and earlier, LTS 2.150.1 and earlier in core/src/main/java/hudson/security/AuthenticationProcessingFilter2.java that allows attackers to extend the duration of active HTTP sessions indefinitely even though the user account may have been deleted in the mean time.
CVE-2019-1003049	Users who cached their CLI authentication before Jenkins was updated to 2.150.2 and newer, or 2.160 and newer, would remain authenticated in Jenkins 2.171 and earlier and Jenkins LTS 2.164.1 and earlier, because the fix for CVE-2019-1003004 in these releases did not reject existing remoting-based CLI authentication caches.
CVE-2019-1003050	The f:validateButton form control for the Jenkins UI did not properly escape job URLs in Jenkins 2.171 and earlier and Jenkins LTS 2.164.1 and earlier, resulting in a cross-site scripting (XSS) vulnerability exploitable by users with the ability to control job names.
CVE-2019-10086	In Apache Commons Beanutils 1.9.2, a special BeanIntrospector class was added which allows suppressing the ability for an attacker to access the classloader via the class property available on all Java objects. We, however were not using this by default characteristic of the PropertyUtilsBean.
CVE-2019-10352	A path traversal vulnerability in Jenkins 2.185 and earlier, LTS 2.176.1 and earlier in core/src/main/java/hudson/model/FileParameterValue.java allowed attackers with Job/Configure permission to define a file parameter with a file name outside the intended directory, resulting in an arbitrary file write on the Jenkins master when scheduling a build.
CVE-2019-10353	CSRF tokens in Jenkins 2.185 and earlier, LTS 2.176.1 and earlier did not expire, thereby allowing attackers able to obtain them to bypass CSRF protection.
CVE-2019-10354	A vulnerability in the Stapler web framework used in Jenkins 2.185 and earlier, LTS 2.176.1 and earlier allowed attackers to access view fragments directly, bypassing permission checks and possibly obtain sensitive information.
CVE-2019-10383	A stored cross-site scripting vulnerability in Jenkins 2.191 and earlier, LTS 2.176.2 and earlier allowed attackers with Overall/Administer permission to configure the update site URL to inject arbitrary HTML and JavaScript in update center web pages.
CVE-2019-10384	Jenkins 2.191 and earlier, LTS 2.176.2 and earlier allowed users to obtain CSRF tokens without an

	associated web session ID, resulting in CSRF tokens that did not expire and could be used to bypass CSRF protection for the anonymous user.
CVE-2019-10401	In Jenkins 2.196 and earlier, LTS 2.176.3 and earlier, the f:expandableTextBox form control interpreted its content as HTML when expanded, resulting in a stored XSS vulnerability exploitable by users with permission to define its contents (typically Job/Configure).
CVE-2019-10402	In Jenkins 2.196 and earlier, LTS 2.176.3 and earlier, the f:combobox form control interpreted its item labels as HTML, resulting in a stored XSS vulnerability exploitable by users with permission to define its contents.
CVE-2019-10403	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier did not escape the SCM tag name on the tooltip for SCM tag actions, resulting in a stored XSS vulnerability exploitable by users able to control SCM tag names for these actions.
CVE-2019-10404	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier did not escape the reason why a queue items is blcoked in tooltips, resulting in a stored XSS vulnerability exploitable by users able to control parts of the reason a queue item is blocked, such as label expressions not matching any idle executors.
CVE-2019-10405	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier printed the value of the "Cookie" HTTP request header on the /whoAmI/ URL, allowing attackers exploiting another XSS vulnerability to obtain the HTTP session cookie despite it being marked HttpOnly.
CVE-2019-10406	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier did not restrict or filter values set as Jenkins URL in the global configuration, resulting in a stored XSS vulnerability exploitable by attackers with Overall/Administer permission.
CVE-2019-11048	In PHP versions 7.2.x below 7.2.31, 7.3.x below 7.3.18 and 7.4.x below 7.4.6, when HTTP file uploads are allowed, supplying overly long filenames or field names could lead PHP engine to try to allocate oversized memory storage, hit the memory limit and stop processing the request, without cleaning up temporary files created by upload request. This potentially could lead to accumulation of uncleaned temporary files exhausting the disk space on the target server.
CVE-2019-11251	The Kubernetes kubectl cp command in versions 1.1-1.12, and versions prior to 1.13.11, 1.14.7, and 1.15.4 allows a combination of two symlinks provided by tar output of a malicious container to place a file outside of the destination directory specified in the kubectl cp invocation. This could be used to allow

	an attacker to place a nefarious file using a symlink, outside of the destination tree.
CVE-2019-11253	Improper input validation in the Kubernetes API server in versions v1.0-1.12 and versions prior to v1.13.12, v1.14.8, v1.15.5, and v1.16.2 allows authorized users to send malicious YAML or JSON payloads, causing the API server to consume excessive CPU or memory, potentially crashing and becoming unavailable. Prior to v1.14.0, default RBAC policy authorized anonymous users to submit requests that could trigger this vulnerability. Clusters upgraded from a version prior to v1.14.0 keep the more permissive policy by default for backwards compatibility.
CVE-2019-12519	An issue was discovered in Squid through 4.7. When handling the tag esi:when when ESI is enabled, Squid calls ESIExpression::Evaluate. This function uses a fixed stack buffer to hold the expression while it's being evaluated. When processing the expression, it could either evaluate the top of the stack, or add a new member to the stack. When adding a new member, there is no check to ensure that the stack won't overflow.
CVE-2019-12521	An issue was discovered in Squid through 4.7. When Squid is parsing ESI, it keeps the ESI elements in ESIContext. ESIContext contains a buffer for holding a stack of ESIElements. When a new ESIElement is parsed, it is added via addStackElement. addStackElement has a check for the number of elements in this buffer, but it's off by 1, leading to a Heap Overflow of 1 element. The overflow is within the same structure so it can't affect adjacent memory blocks, and thus just leads to a crash while processing.
CVE-2019-12815	An arbitrary file copy vulnerability in mod_copy in ProFTPD up to 1.3.5b allows for remote code execution and information disclosure without authentication, a related issue to CVE-2015-3306.
CVE-2019-12900	BZ2_decompress in decompress.c in bzip2 through 1.0.6 has an out-of-bounds write when there are many selectors.
CVE-2019-13117	In numbers.c in libxslt 1.1.33, an xsl:number with certain format strings could lead to a uninitialized read in xsltNumberFormatInsertNumbers. This could allow an attacker to discern whether a byte on the stack contains the characters A, a, I, i, or 0, or any other character.
CVE-2019-13118	In numbers.c in libxslt 1.1.33, a type holding grouping characters of an xsl:number instruction was too narrow and an invalid character/length combination could be passed to xsltNumberFormatDecimal, leading to a read of uninitialized stack data.

CVE-2019-13312	block_cmp() in libavcodec/zmbvenc.c in FFmpeg 4.1.3 has a heap-based buffer over-read.
CVE-2019-13659	IDN spoofing in Omnibox in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2019-13660	UI spoofing in Chromium in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof notifications via a crafted HTML page.
CVE-2019-13661	UI spoofing in Chromium in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof notifications via a crafted HTML page.
CVE-2019-13662	Insufficient policy enforcement in navigations in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2019-13663	IDN spoofing in Omnibox in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2019-13664	Insufficient policy enforcement in Blink in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2019-13665	Insufficient filtering in Blink in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass multiple file download protection via a crafted HTML page.
CVE-2019-13666	Information leak in storage in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13667	Inappropriate implementation in Omnibox in Google Chrome on iOS prior to 77.0.3865.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-13668	Insufficient policy enforcement in developer tools in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13669	Incorrect data validation in navigation in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-13670	Insufficient data validation in JavaScript in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2019-13671	UI spoofing in Blink in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2019-13673	Insufficient data validation in developer tools in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13674	IDN spoofing in Omnibox in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2019-13675	Insufficient data validation in extensions in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to disable extensions via a crafted HTML page.
CVE-2019-13676	Insufficient policy enforcement in Chromium in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2019-13677	Insufficient policy enforcement in site isolation in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2019-13678	Incorrect data validation in downloads in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2019-13679	Insufficient policy enforcement in PDFium in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to show print dialogs via a crafted PDF file.
CVE-2019-13680	Inappropriate implementation in TLS in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof client IP address to websites via crafted TLS connections.
CVE-2019-13681	Insufficient data validation in downloads in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass download restrictions via a crafted HTML page.
CVE-2019-13682	Insufficient policy enforcement in external protocol handling in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass same origin policy via a crafted HTML page.
CVE-2019-13683	Insufficient policy enforcement in developer tools in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13685	Use after free in sharing view in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13686	Use after free in offline mode in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2019-13687	Use after free in Blink in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13688	Use after free in Blink in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13693	Use after free in IndexedDB in Google Chrome prior to 77.0.3865.120 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page.
CVE-2019-13694	Use after free in WebRTC in Google Chrome prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13695	Use after free in audio in Google Chrome on Android prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13696	Use after free in JavaScript in Google Chrome prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13697	Insufficient policy enforcement in performance APIs in Google Chrome prior to 77.0.3865.120 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13699	Use after free in media in Google Chrome prior to 78.0.3904.70 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13700	Out of bounds memory access in the gamepad API in Google Chrome prior to 78.0.3904.70 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13701	Incorrect implementation in navigation in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-13702	Inappropriate implementation in installer in Google Chrome on Windows prior to 78.0.3904.70 allowed a local attacker to perform privilege escalation via a crafted executable.
CVE-2019-13703	Insufficient policy enforcement in the Omnibox in Google Chrome on Android prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-13704	Insufficient policy enforcement in navigation in Google Chrome prior to 78.0.3904.70 allowed a remote attacker

	to bypass content security policy via a crafted HTML page.
CVE-2019-13705	Insufficient policy enforcement in extensions in Google Chrome prior to 78.0.3904.70 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension.
CVE-2019-13706	Out of bounds memory access in PDFium in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-13707	Insufficient validation of untrusted input in intents in Google Chrome on Android prior to 78.0.3904.70 allowed a local attacker to leak files via a crafted application.
CVE-2019-13708	Inappropriate implementation in navigation in Google Chrome on iOS prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-13709	Insufficient policy enforcement in downloads in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to bypass download restrictions via a crafted HTML page.
CVE-2019-13710	Insufficient validation of untrusted input in downloads in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to bypass download restrictions via a crafted HTML page.
CVE-2019-13711	Insufficient policy enforcement in JavaScript in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13713	Insufficient policy enforcement in JavaScript in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13714	Insufficient validation of untrusted input in Color Enhancer extension in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to inject CSS into an HTML page via a crafted URL.
CVE-2019-13715	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2019-13716	Insufficient policy enforcement in service workers in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2019-13717	Incorrect security UI in full screen mode in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to hide security UI via a crafted HTML page.

CVE-2019-13718	Insufficient data validation in Omnibox in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2019-13719	Incorrect security UI in full screen mode in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to hide security UI via a crafted HTML page.
CVE-2019-13720	Use after free in WebAudio in Google Chrome prior to 78.0.3904.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13721	Use after free in PDFium in Google Chrome prior to 78.0.3904.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13723	Use after free in WebBluetooth in Google Chrome prior to 78.0.3904.108 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13724	Out of bounds memory access in WebBluetooth in Google Chrome prior to 78.0.3904.108 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13725	Use-after-free in Bluetooth in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2019-13726	Buffer overflow in password manager in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2019-13727	Insufficient policy enforcement in WebSockets in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to bypass same origin policy via a crafted HTML page.
CVE-2019-13728	Out of bounds write in JavaScript in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13729	Use-after-free in WebSockets in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13730	Type confusion in JavaScript in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13732	Use-after-free in WebAudio in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13734	Out of bounds write in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2019-13735	Out of bounds write in JavaScript in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2019-13736	Integer overflow in PDFium in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-13737	Insufficient policy enforcement in autocomplete in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-13738	Insufficient policy enforcement in navigation in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2019-13739	Insufficient policy enforcement in Omnibox in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2019-13740	Incorrect security UI in sharing in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2019-13741	Insufficient validation of untrusted input in Blink in Google Chrome prior to 79.0.3945.79 allowed a local attacker to bypass same origin policy via crafted clipboard content.
CVE-2019-13742	Incorrect security UI in Omnibox in Google Chrome on iOS prior to 79.0.3945.79 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2019-13743	Incorrect security UI in external protocol handling in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2019-13744	Insufficient policy enforcement in cookies in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13745	Insufficient policy enforcement in audio in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13746	Insufficient policy enforcement in Omnibox in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-13747	Uninitialized data in rendering in Google Chrome on Android prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13748	Insufficient policy enforcement in developer tools in Google Chrome prior to 79.0.3945.79 allowed a local

	attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-13749	Incorrect security UI in Omnibox in Google Chrome on iOS prior to 79.0.3945.79 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-13750	Insufficient data validation in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to bypass defense-in-depth measures via a crafted HTML page.
CVE-2019-13751	Uninitialized data in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-13752	Out of bounds read in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-13753	Out of bounds read in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-13754	Insufficient policy enforcement in extensions in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2019-13755	Insufficient policy enforcement in extensions in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to disable extensions via a crafted HTML page.
CVE-2019-13756	Incorrect security UI in printing in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2019-13757	Incorrect security UI in Omnibox in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2019-13758	Insufficient policy enforcement in navigation in Google Chrome on Android prior to 79.0.3945.79 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2019-13759	Incorrect security UI in interstitials in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2019-13761	Incorrect security UI in Omnibox in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.

CVE-2019-13762	Insufficient policy enforcement in downloads in Google Chrome on Windows prior to 79.0.3945.79 allowed a local attacker to spoof downloaded files via local code.
CVE-2019-13763	Insufficient policy enforcement in payments in Google Chrome prior to 79.0.3945.79 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page.
CVE-2019-13764	Type confusion in JavaScript in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13765	Use-after-free in content delivery manager in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13766	Use-after-free in accessibility in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13767	Use after free in media picker in Google Chrome prior to 79.0.3945.88 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-14562	Integer overflow in DxeImageVerificationHandler() EDK II may allow an authenticated user to potentially enable denial of service via local access.
CVE-2019-14834	A vulnerability was found in dnsmasq before version 2.81, where the memory leak allows remote attackers to cause a denial of service (memory consumption) via vectors involving DHCP response creation.
CVE-2019-15680	TightVNC code version 1.3.10 contains null pointer dereference in HandleZlibBPP function, which results Denial of System (DoS). This attack appear to be exploitable via network connectivity.
CVE-2019-15681	LibVNC commit before d01e1bb4246323ba6fcee3b82ef1faa9b1dac82a contains a memory leak (CWE-655) in VNC server code, which allow an attacker to read stack memory and can be abused for information disclosure. Combined with another vulnerability, it can be used to leak stack memory and bypass ASLR. This attack appear to be exploitable via network connectivity. These vulnerabilities have been fixed in commit d01e1bb4246323ba6fcee3b82ef1faa9b1dac82a.
CVE-2019-16089	An issue was discovered in the Linux kernel through 5.2.13. nbd_genl_status in drivers/block/nbd.c does not check the nla_nest_start_noflag return value.
CVE-2019-16168	In SQLite through 3.29.0, whereLoopAddBtreeIndex in sqlite3.c can crash a browser or other application because of missing validation of a sqlite_stat1 sz field, aka a "severe division by zero in the query planner."

CVE-2019-16276	Go before 1.12.10 and 1.13.x before 1.13.1 allow HTTP Request Smuggling.
CVE-2019-16943	A Polymorphic Typing issue was discovered in FasterXML jackson-databind 2.0.0 through 2.9.10. When Default Typing is enabled (either globally or for a specific property) for an externally exposed JSON endpoint and the service has the p6spy (3.8.6) jar in the classpath, and an attacker can find an RMI service endpoint to access, it is possible to make the service execute a malicious payload. This issue exists because of com.p6spy.engine.spy.P6DataSource mishandling.
CVE-2019-17023	After a HelloRetryRequest has been sent, the client may negotiate a lower protocol that TLS 1.3, resulting in an invalid state transition in the TLS State Machine. If the client gets into this state, incoming Application Data records will be ignored. This vulnerability affects Firefox < 72.
CVE-2019-17177	libfreerdp/codec/region.c in FreeRDP through 1.1.x and 2.x through 2.0.0-rc4 has memory leaks because a supplied realloc pointer (i.e., the first argument to realloc) is also used for a realloc return value.
CVE-2019-17195	Connect2id Nimbus JOSE+JWT before v7.9 can throw various uncaught exceptions while parsing a JWT, which could result in an application crash (potential information disclosure) or a potential authentication bypass.
CVE-2019-17267	A Polymorphic Typing issue was discovered in FasterXML jackson-databind before 2.9.10. It is related to net.sf.ehcache.hibernate.EhcacheJtaTransactionManagerLookup.
CVE-2019-17359	The ASN.1 parser in Bouncy Castle Crypto (aka BC Java) 1.63 can trigger a large attempted memory allocation, and resultant OutOfMemoryError error, via crafted ASN.1 data. This is fixed in 1.64.
CVE-2019-17514	library/glob.html in the Python 2 and 3 documentation before 2016 has potentially misleading information about whether sorting occurs, as demonstrated by irreproducible cancer-research results. NOTE: the effects of this documentation cross application domains, and thus it is likely that security-relevant code elsewhere is affected. This issue is not a Python implementation bug, and there are no reports that NMR researchers were specifically relying on library/glob.html. In other words, because the older documentation stated "finds all the pathnames matching a specified pattern according to the rules used by the Unix shell," one might have incorrectly inferred that the sorting that occurs in a Unix shell also occurred for glob.glob. There is a workaround in newer versions

	of Willoughby nmr-data_compilation-p2.py and nmr-data_compilation-p3.py, which call sort() directly.
CVE-2019-17571	Included in Log4j 1.2 is a SocketServer class that is vulnerable to deserialization of untrusted data which can be exploited to remotely execute arbitrary code when combined with a deserialization gadget when listening to untrusted network traffic for log data. This affects Log4j versions up to 1.2 up to 1.2.17.
CVE-2019-17638	In Eclipse Jetty, versions 9.4.27.v20200227 to 9.4.29.v20200521, in case of too large response headers, Jetty throws an exception to produce an HTTP 431 error. When this happens, the ByteBuffer containing the HTTP response headers is released back to the ByteBufferPool twice. Because of this double release, two threads can acquire the same ByteBuffer from the pool and while thread1 is about to use the ByteBuffer to write response1 data, thread2 fills the ByteBuffer with other data. Thread1 then proceeds to write the buffer that now contains different data. This results in client1, which issued request1 seeing data from another request or response which could contain sensitive data belonging to client2 (HTTP session ids, authentication credentials, etc.). If the Jetty version cannot be upgraded, the vulnerability can be significantly reduced by configuring a responseHeaderSize significantly larger than the requestHeaderSize (12KB responseHeaderSize and 8KB requestHeaderSize).
CVE-2019-18197	In xsltCopyText in transform.c in libxslt 1.1.33, a pointer variable isn't reset under certain circumstances. If the relevant memory area happened to be freed and reused in a certain way, a bounds check could fail and memory outside a buffer could be written to, or uninitialized data could be disclosed.
CVE-2019-18348	An issue was discovered in urllib2 in Python 2.x through 2.7.17 and urllib in Python 3.x through 3.8.0. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the host component of a URL) followed by an HTTP header. This is similar to the CVE-2019-9740 query string issue and the CVE-2019-9947 path string issue. (This is not exploitable when glibc has CVE-2016-10739 fixed.). This is fixed in: v2.7.18, v2.7.18rc1; v3.5.10, v3.5.10rc1; v3.6.11, v3.6.11rc1, v3.6.12; v3.7.8, v3.7.8rc1, v3.7.9; v3.8.3, v3.8.3rc1, v3.8.4, v3.8.4rc1, v3.8.5, v3.8.6, v3.8.6rc1.
CVE-2019-18808	A memory leak in the ccp_run_sha_cmd() function in drivers/crypto/ccp/ccp-ops.c in the Linux kernel through 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-128c66429247.

CVE-2019-19054	A memory leak in the cx23888_ir_probe() function in drivers/media/pci/cx23885/cx23888-ir.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering kfifo_alloc() failures, aka CID-a7b2df76b42b.
CVE-2019-19377	In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image, performing some operations, and unmounting can lead to a use-after-free in btrfs_queue_work in fs/btrfs/async-thread.c.
CVE-2019-19462	relay_open in kernel/relay.c in the Linux kernel through 5.4.1 allows local users to cause a denial of service (such as relay blockage) by triggering a NULL alloc_percpu result.
CVE-2019-19880	exprListAppendList in window.c in SQLite 3.30.1 allows attackers to trigger an invalid pointer dereference because constant integer values in ORDER BY clauses of window definitions are mishandled.
CVE-2019-19923	flattenSubquery in select.c in SQLite 3.30.1 mishandles certain uses of SELECT DISTINCT involving a LEFT JOIN in which the right-hand side is a view. This can cause a NULL pointer dereference (or incorrect results).
CVE-2019-19925	zipfileUpdate in ext/misc/zipfile.c in SQLite 3.30.1 mishandles a NULL pathname during an update of a ZIP archive.
CVE-2019-19926	multiSelect in select.c in SQLite 3.30.1 mishandles certain errors during parsing, as demonstrated by errors from sqlite3WindowRewrite() calls. NOTE: this vulnerability exists because of an incomplete fix for CVE-2019-19880.
CVE-2019-19948	In ImageMagick 7.0.8-43 Q16, there is a heap-based buffer overflow in the function WriteSGIImage of coders/sgi.c.
CVE-2019-19949	In ImageMagick 7.0.8-43 Q16, there is a heap-based buffer over-read in the function WritePNGImage of coders/png.c, related to Magick_png_write_raw_profile and LocaleNCompare.
CVE-2019-20373	LTSP LDM through 2.18.06 allows fat-client root access because the LDM_USERNAME variable may have an empty value if the user's shell lacks support for Bourne shell syntax. This is related to a run-x-session script.
CVE-2019-20503	usrsctp before 2019-12-20 has out-of-bounds reads in sctp_load_addresses_from_init.
CVE-2019-20810	go7007_snd_init in drivers/media/usb/go7007/snd-go7007.c in the Linux kernel before 5.6 does not call snd_card_free for a failure path, which causes a memory leak, aka CID-9453264ef586.
CVE-2019-20839	libvncclient/sockets.c in LibVNCServer before 0.9.13 has a buffer overflow via a long socket filename.

CVE-2019-20892	net-snmp before 5.8.1.pre1 has a double free in usm_free_usmStateReference in snmplib/snmpusm.c via an SNMPv3 GetBulk request. NOTE: this affects net-snmp packages shipped to end users by multiple Linux distributions, but might not affect an upstream release.
CVE-2019-20907	In Lib/tarfile.py in Python through 3.8.3, an attacker is able to craft a TAR archive leading to an infinite loop when opened by tarfile.open, because _proc_pax lacks header validation.
CVE-2019-2395	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). The supported version that is affected is 10.3.6.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.0 Base Score 5.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L).
CVE-2019-2398	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Deployment). Supported versions that are affected are 10.3.6.0, 12.1.3.0 and 12.2.1.3. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2019-2418	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0, 12.1.3.0 and 12.2.1.3. Difficult to exploit vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. While the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.0 Base Score 6.5 (Confidentiality, Integrity and Availability impacts).

	CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:L/I:L/A:L).
CVE-2019-2422	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u201, 8u192 and 11.0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).
CVE-2019-2426	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 7u201, 8u192 and 11.0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2019-2441	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Application Container - JavaEE). The supported version that is affected is 12.2.1.3. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts).

	CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2019-2449	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). The supported version that is affected is Java SE: 8u192. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L).
CVE-2019-2452	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0, 12.1.3.0 and 12.2.1.3. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.0 Base Score 6.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:H/A:H).
CVE-2019-2568	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. While the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.0 (Integrity

	impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:L/A:N).
CVE-2019-2602	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2019-2615	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).
CVE-2019-2618	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data as well as unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N).
CVE-2019-2645	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this

	vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2019-2646	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: EJB Container). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2019-2647	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2019-2648	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2019-2649	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).

CVE-2019-2650	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS - Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2019-2658	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2019-2684	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).
CVE-2019-2697	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 7u211 and 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running

	sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2019-2698	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 7u211 and 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2019-2725	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2019-2729	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2019-2745	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that

	are affected are Java SE: 7u221, 8u212 and 11.0.3. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE executes to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2019-2762	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Utilities). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2766	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load

	and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).
CVE-2019-2769	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Utilities). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2786	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N).

CVE-2019-2816	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2019-2818	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 11.0.3 and 12.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).
CVE-2019-2821	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JSSE). Supported versions that are affected are Java SE: 11.0.3 and 12.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability applies to Java

	deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N).
CVE-2019-2824	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data as well as unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N).
CVE-2019-2827	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0 and 12.2.1.3.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data as well as unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N).
CVE-2019-2842	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JCE). The supported version that is affected is Java SE: 8u212. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the

	specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2853	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).
CVE-2019-2856	Vulnerability in the Oracle WebLogic Server component of Oracle Fusion Middleware (subcomponent: Application Container - JavaEE). Supported versions that are affected is 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2019-3689	The nfs-utils package in SUSE Linux Enterprise Server 12 before and including version 1.3.0-34.18.1 and in SUSE Linux Enterprise Server 15 before and including version 2.1.1-6.10.2 the directory /var/lib/nfs is owned by statd:nogroup. This directory contains files owned and managed by root. If statd is compromised, it can therefore trick processes running with root privileges into creating/overwriting files anywhere on the system.
CVE-2019-4014	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force ID: 155892.

CVE-2019-4015	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-ForceID: 155893.
CVE-2019-4016	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-ForceID: 155894.
CVE-2019-4030	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 155946.
CVE-2019-4057	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 could allow malicious user with access to the DB2 instance account to leverage a fenced execution process to execute arbitrary code as root. IBM X-Force ID: 156567.
CVE-2019-4094	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 binaries load shared libraries from an untrusted path potentially giving low privilege user full access to root by loading a malicious shared library. IBM X-Force ID: 158014.
CVE-2019-4101	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 10.1, 10.5, and 11.1 is vulnerable to a denial of service. Users that have both EXECUTE on PD_GET_DIAG_HIST and access to the diagnostic directory on the DB2 server can cause the instance to crash. IBM X-Force ID: 158091.
CVE-2019-4102	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 158092.
CVE-2019-4154	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force ID: 158519.
CVE-2019-4270	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Admin Console is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 160203.

CVE-2019-4271	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Admin console is vulnerable to a Client-side HTTP parameter pollution vulnerability. IBM X-Force ID: 160243.
CVE-2019-4279	IBM WebSphere Application Server 8.5 and 9.0 could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects from untrusted sources. IBM X-Force ID: 160445.
CVE-2019-4322	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force ID: 161202.
CVE-2019-4386	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1 could allow an authenticated user to execute a function that would cause the server to crash. IBM X-Force ID: 162714.
CVE-2019-4441	IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0, and Liberty could allow a remote attacker to obtain sensitive information when a stack trace is returned in the browser. IBM X-Force ID: 163177.
CVE-2019-4442	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9,0 could allow a remote attacker to traverse directories on the file system. An attacker could send a specially-crafted URL request to view arbitrary files on the system but not content. IBM X-Force ID: 163226.
CVE-2019-4477	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a user with access to audit logs to obtain sensitive information, caused by improper handling of command line options. IBM X-Force ID: 163997.
CVE-2019-4505	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Network Deployment could allow a remote attacker to obtain sensitive information, caused by sending a specially-crafted URL. This can lead the attacker to view any file in a certain directory. IBM X-Force ID: 164364.
CVE-2019-5527	ESXi, Workstation, Fusion, VMRC and Horizon Client contain a use-after-free vulnerability in the virtual sound device. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 8.5.
CVE-2019-5754	Implementation error in QUIC Networking in Google Chrome prior to 72.0.3626.81 allowed an attacker running or able to cause use of a proxy server to obtain cleartext of transport encryption via malicious network proxy.

CVE-2019-5755	Incorrect handling of negative zero in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page.
CVE-2019-5756	Inappropriate memory management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.
CVE-2019-5757	An incorrect object type assumption in SVG in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2019-5758	Incorrect object lifecycle management in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5759	Incorrect lifetime handling in HTML select elements in Google Chrome on Android and Mac prior to 72.0.3626.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2019-5760	Insufficient checks of pointer validity in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5761	Incorrect object lifecycle management in SwiftShader in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5762	Inappropriate memory management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.
CVE-2019-5763	Failure to check error conditions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5764	Incorrect pointer management in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5765	An exposed debugging endpoint in the browser in Google Chrome on Android prior to 72.0.3626.81 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted Intent.
CVE-2019-5766	Incorrect handling of origin taint checking in Canvas in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-5767	Insufficient protection of permission UI in WebAPKs in Google Chrome on Android prior to 72.0.3626.81

	allowed an attacker who convinced the user to install a malicious application to access privacy/security sensitive web APIs via a crafted APK.
CVE-2019-5768	DevTools API not correctly gating on extension capability in DevTools in Google Chrome prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to read local files via a crafted Chrome Extension.
CVE-2019-5769	Incorrect handling of invalid end character position when front rendering in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5770	Insufficient input validation in WebGL in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2019-5771	An incorrect JIT of GLSL shaders in SwiftShader in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2019-5772	Sharing of objects over calls into JavaScript runtime in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5773	Insufficient origin validation in IndexedDB in Google Chrome prior to 72.0.3626.81 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page.
CVE-2019-5774	Omission of the .desktop filetype from the Safe Browsing checklist in SafeBrowsing in Google Chrome on Linux prior to 72.0.3626.81 allowed an attacker who convinced a user to download a .desktop file to execute arbitrary code via a downloaded .desktop file.
CVE-2019-5775	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2019-5776	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2019-5777	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2019-5778	A missing case for handling special schemes in permission request checks in Extensions in Google Chrome prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to

	bypass extension permission checks for privileged pages via a crafted Chrome Extension.
CVE-2019-5779	Insufficient policy validation in ServiceWorker in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2019-5780	Insufficient restrictions on what can be done with Apple Events in Google Chrome on macOS prior to 72.0.3626.81 allowed a local attacker to execute JavaScript via Apple Events.
CVE-2019-5781	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2019-5782	Incorrect optimization assumptions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2019-5783	Missing URI encoding of untrusted input in DevTools in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform a Dangling Markup Injection attack via a crafted HTML page.
CVE-2019-5784	Incorrect handling of deferred code in V8 in Google Chrome prior to 72.0.3626.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5786	Object lifetime issue in Blink in Google Chrome prior to 72.0.3626.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2019-5787	Use-after-garbage-collection in Blink in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5788	An integer overflow that leads to a use-after-free in Blink Storage in Google Chrome on Linux prior to 73.0.3683.75 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page.
CVE-2019-5789	An integer overflow that leads to a use-after-free in WebMIDI in Google Chrome on Windows prior to 73.0.3683.75 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page.
CVE-2019-5790	An integer overflow leading to an incorrect capacity of a buffer in JavaScript in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.

CVE-2019-5791	Inappropriate optimization in V8 in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2019-5792	Integer overflow in PDFium in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially perform out of bounds memory access via a crafted PDF file.
CVE-2019-5793	Insufficient policy enforcement in extensions in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to initiate the extensions installation user interface via a crafted HTML page.
CVE-2019-5794	Incorrect handling of cancelled requests in Navigation in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2019-5795	Integer overflow in PDFium in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially perform out of bounds memory access via a crafted PDF file.
CVE-2019-5796	Data race in extensions guest view in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5798	Lack of correct bounds checking in Skia in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2019-5799	Incorrect inheritance of a new document's policy in Content Security Policy in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2019-5800	Insufficient policy enforcement in Blink in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2019-5802	Incorrect handling of download origins in Navigation in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2019-5803	Insufficient policy enforcement in Content Security Policy in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2019-5805	Use-after-free in PDFium in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5806	Integer overflow in ANGLE in Google Chrome on Windows prior to 74.0.3729.108 allowed a remote

	attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5807	Object lifetime issue in V8 in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5808	Use after free in Blink in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5809	Use after free in file chooser in Google Chrome prior to 74.0.3729.108 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page.
CVE-2019-5810	Information leak in autofill in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-5811	Incorrect handling of CORS in ServiceWorker in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass same origin policy via a crafted HTML page.
CVE-2019-5813	Use after free in V8 in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5814	Insufficient policy enforcement in Blink in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-5815	Type confusion in xsltNumberFormatGetMultipleLevel prior to libxslt 1.1.33 could allow attackers to potentially exploit heap corruption via crafted XML data.
CVE-2019-5818	Uninitialized data in media in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted video file.
CVE-2019-5819	Insufficient data validation in developer tools in Google Chrome on OS X prior to 74.0.3729.108 allowed a local attacker to execute arbitrary code via a crafted string copied to clipboard.
CVE-2019-5820	Integer overflow in PDFium in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5821	Integer overflow in PDFium in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5822	Inappropriate implementation in Blink in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass same origin policy via a crafted HTML page.

CVE-2019-5823	Insufficient policy enforcement in service workers in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2019-5824	Parameter passing error in media in Google Chrome prior to 74.0.3729.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5825	Out of bounds write in JavaScript in Google Chrome prior to 73.0.3683.86 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5826	Use after free in IndexedDB in Google Chrome prior to 73.0.3683.86 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5827	Integer overflow in SQLite via WebSQL in Google Chrome prior to 74.0.3729.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5828	Object lifecycle issue in ServiceWorker in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2019-5829	Integer overflow in download manager in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2019-5830	Insufficient policy enforcement in CORS in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-5831	Object lifecycle issue in V8 in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5832	Insufficient policy enforcement in XMLHttpRequest in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-5833	Incorrect dialog box scoping in browser in Google Chrome on Android prior to 75.0.3770.80 allowed a remote attacker to display misleading security UI via a crafted HTML page.
CVE-2019-5835	Object lifecycle issue in SwiftShader in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.

CVE-2019-5836	Heap buffer overflow in ANGLE in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5837	Resource size information leakage in Blink in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-5838	Insufficient policy enforcement in extensions API in Google Chrome prior to 75.0.3770.80 allowed an attacker who convinced a user to install a malicious extension to bypass restrictions on file URIs via a crafted Chrome Extension.
CVE-2019-5839	Excessive data validation in URL parser in Google Chrome prior to 75.0.3770.80 allowed a remote attacker who convinced a user to input a URL to bypass website URL validation via a crafted URL.
CVE-2019-5840	Incorrect security UI in popup blocker in Google Chrome on iOS prior to 75.0.3770.80 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2019-5842	Use after free in Blink in Google Chrome prior to 75.0.3770.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5844	Out of bounds access in SwiftShader in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5845	Out of bounds access in SwiftShader in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5846	Out of bounds access in SwiftShader in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5847	Inappropriate implementation in JavaScript in Google Chrome prior to 75.0.3770.142 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5848	Incorrect font handling in autofill in Google Chrome prior to 75.0.3770.142 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-5850	Use after free in offline mode in Google Chrome prior to 76.0.3809.87 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.

CVE-2019-5851	Use after free in WebAudio in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5852	Inappropriate implementation in JavaScript in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-5853	Inappropriate implementation in JavaScript in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5854	Integer overflow in PDFium in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5855	Integer overflow in PDFium in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5856	Insufficient policy enforcement in storage in Google Chrome prior to 76.0.3809.87 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.
CVE-2019-5857	Inappropriate implementation in JavaScript in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2019-5858	Incorrect security UI in MacOS services integration in Google Chrome on OS X prior to 76.0.3809.87 allowed a local attacker to execute arbitrary code via a crafted HTML page.
CVE-2019-5859	Insufficient filtering in URI schemes in Google Chrome on Windows prior to 76.0.3809.87 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2019-5860	Use after free in PDFium in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5861	Insufficient data validation in Blink in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to bypass anti-clickjacking policy via a crafted HTML page.
CVE-2019-5862	Insufficient data validation in AppCache in Google Chrome prior to 76.0.3809.87 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.
CVE-2019-5864	Insufficient data validation in CORS in Google Chrome prior to 76.0.3809.87 allowed an attacker who convinced a user to install a malicious extension to bypass content security policy via a crafted Chrome Extension.

CVE-2019-5865	Insufficient policy enforcement in navigations in Google Chrome prior to 76.0.3809.87 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.
CVE-2019-5867	Out of bounds read in JavaScript in Google Chrome prior to 76.0.3809.100 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5868	Use after free in PDFium in Google Chrome prior to 76.0.3809.100 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5869	Use after free in Blink in Google Chrome prior to 76.0.3809.132 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5870	Use after free in media in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2019-5871	Heap buffer overflow in Skia in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5872	Use after free in Mojo in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5874	Insufficient filtering in URI schemes in Google Chrome on Windows prior to 77.0.3865.75 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2019-5875	Insufficient data validation in downloads in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-5876	Use after free in media in Google Chrome on Android prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5877	Out of bounds memory access in JavaScript in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5878	Use after free in V8 in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5879	Insufficient policy enforcement in extensions in Google Chrome prior to 77.0.3865.75 allowed an attacker who convinced a user to install a malicious extension to read local files via a crafted Chrome Extension.

CVE-2019-5880	Insufficient policy enforcement in Blink in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-5881	Out of bounds read in SwiftShader in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-7090	Flash Player Desktop Runtime versions 32.0.0.114 and earlier, Flash Player for Google Chrome versions 32.0.0.114 and earlier, and Flash Player for Microsoft Edge and Internet Explorer 11 versions 32.0.0.114 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2019-7096	Adobe Flash Player versions 32.0.0.156 and earlier, 32.0.0.156 and earlier, and 32.0.0.156 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2019-7108	Adobe Flash Player versions 32.0.0.156 and earlier, 32.0.0.156 and earlier, and 32.0.0.156 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .
CVE-2019-7317	png_image_free in png.c in libpng 1.6.x before 1.6.37 has a use-after-free because png_image_free_function is called under png_safe_execute.
CVE-2019-7608	Kibana versions before 5.6.15 and 6.6.1 had a cross-site scripting (XSS) vulnerability that could allow an attacker to obtain sensitive information from or perform destructive actions on behalf of other Kibana users.
CVE-2019-7609	Kibana versions before 5.6.15 and 6.6.1 contain an arbitrary code execution flaw in the Timelion visualizer. An attacker with access to the Timelion application could send a request that will attempt to execute javascript code. This could possibly lead to an attacker executing arbitrary commands with permissions of the Kibana process on the host system.
CVE-2019-7610	Kibana versions before 6.6.1 contain an arbitrary code execution flaw in the security audit logger. If a Kibana instance has the setting xpack.security.audit.enabled set to true, an attacker could send a request that will attempt to execute javascript code. This could possibly lead to an attacker executing arbitrary commands with permissions of the Kibana process on the host system.
CVE-2019-7614	A race condition flaw was found in the response headers Elasticsearch versions before 7.2.1 and 6.8.2 returns to a request. On a system with multiple users submitting requests, it could be possible for an attacker to gain access to response header containing sensitive data from another user.

CVE-2019-7616	Kibana versions before 6.8.2 and 7.2.1 contain a server side request forgery (SSRF) flaw in the graphite integration for Timelion visualizer. An attacker with administrative Kibana access could set the timelion:graphite.url configuration option to an arbitrary URL. This could possibly lead to an attacker accessing external URL resources as the Kibana process on the host system.
CVE-2019-7619	Elasticsearch versions 7.0.0-7.3.2 and 6.7.0-6.8.3 contain a username disclosure flaw was found in the API Key service. An unauthenticated attacker could send a specially crafted request and determine if a username exists in the Elasticsearch native realm.
CVE-2019-7621	Kibana versions before 6.8.6 and 7.5.1 contain a cross site scripting (XSS) flaw in the coordinate and region map visualizations. An attacker with the ability to create coordinate map visualizations could create a malicious visualization. If another Kibana user views that visualization or a dashboard containing the visualization it could execute JavaScript in the victimï¿½s browser.
CVE-2019-7652	TheHive Project UnshortenLink analyzer before 1.1, included in Cortex-Analyzers before 1.15.2, has SSRF. To exploit the vulnerability, an attacker must create a new analysis, select URL for Data Type, and provide an SSRF payload like "http://127.0.0.1:22" in the Data parameter. The result can be seen in the main dashboard. Thus, it is possible to do port scans on localhost and intranet hosts.
CVE-2019-7837	Adobe Flash Player versions 32.0.0.171 and earlier, 32.0.0.171 and earlier, and 32.0.0.171 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2019-7845	Adobe Flash Player versions 32.0.0.192 and earlier, 32.0.0.192 and earlier, and 32.0.0.192 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2019-8069	Adobe Flash Player 32.0.0.238 and earlier versions, 32.0.0.207 and earlier versions have a Same Origin Method Execution vulnerability. Successful exploitation could lead to Arbitrary Code Execution in the context of the current user.
CVE-2019-8070	Adobe Flash Player 32.0.0.238 and earlier versions, 32.0.0.207 and earlier versions have a Use after free vulnerability. Successful exploitation could lead to Arbitrary Code Execution in the context of the current user.
CVE-2019-8075	Adobe Flash Player version 32.0.0.192 and earlier versions have a Same Origin Policy Bypass vulnerability. Successful exploitation could lead to

	Information Disclosure in the context of the current user.
CVE-2019-9512	Some HTTP/2 implementations are vulnerable to ping floods, potentially leading to a denial of service. The attacker sends continual pings to an HTTP/2 peer, causing the peer to build an internal queue of responses. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both.
CVE-2019-9514	Some HTTP/2 implementations are vulnerable to a reset flood, potentially leading to a denial of service. The attacker opens a number of streams and sends an invalid request over each stream that should solicit a stream of RST_STREAM frames from the peer. Depending on how the peer queues the RST_STREAM frames, this can consume excess memory, CPU, or both.
CVE-2019-9674	Lib/zipfile.py in Python through 3.7.2 allows remote attackers to cause a denial of service (resource consumption) via a ZIP bomb.
CVE-2019-9923	pax_decode_header in sparse.c in GNU Tar before 1.32 had a NULL pointer dereference when parsing certain archives that have malformed extended headers.
CVE-2020-0067	In f2fs_xattr_generic_list of xattr.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not required for exploitation.Product: Android. Versions: Android kernel. Android ID: A-120551147.
CVE-2020-0093	In exif_data_save_data_entry of exif-data.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-148705132
CVE-2020-0182	In exif_entry_get_value of exif-entry.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-147140917
CVE-2020-0198	In exif_data_load_data_content of exif-data.c, there is a possible UBSAN abort due to an integer overflow. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-146428941

CVE-2020-0423	In binder_release_work of binder.c, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-161151868References: N/A
CVE-2020-0452	In exif_entry_get_value of exif-entry.c, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution if a third party app used this library to process remote image data with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11 Android-8.0Android ID: A-159625731
CVE-2020-0543	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2020-0548	Cleanup errors in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2020-0549	Cleanup errors in some data cache evictions for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2020-10135	Legacy pairing and secure-connections pairing authentication in Bluetooth BR/EDR Core Specification v5.2 and earlier may allow an unauthenticated user to complete authentication without pairing credentials via adjacent access. An unauthenticated, adjacent attacker could impersonate a Bluetooth BR/EDR master or slave to pair with a previously paired remote device to successfully complete the authentication procedure without knowing the link key.
CVE-2020-10177	Pillow before 7.1.0 has multiple out-of-bounds reads in libImaging/FliDecode.c.
CVE-2020-10378	In libImaging/PcxDecode.c in Pillow before 7.1.0, an out-of-bounds read can occur when reading PCX files where state->shuffle is instructed to read beyond state->buffer.
CVE-2020-10379	In Pillow before 7.1.0, there are two Buffer Overflows in libImaging/TiffDecode.c.
CVE-2020-10543	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.
CVE-2020-10700	A use-after-free flaw was found in the way samba AD DC LDAP servers, handled 'Paged Results' control is combined with the 'ASQ' control. A malicious user

	in a samba AD could use this flaw to cause denial of service. This issue affects all samba versions before 4.10.15, before 4.11.8 and before 4.12.2.
CVE-2020-10704	A flaw was found when using samba as an Active Directory Domain Controller. Due to the way samba handles certain requests as an Active Directory Domain Controller LDAP server, an unauthorized user can cause a stack overflow leading to a denial of service. The highest threat from this vulnerability is to system availability. This issue affects all samba versions before 4.10.15, before 4.11.8 and before 4.12.2.
CVE-2020-10711	A NULL pointer dereference flaw was found in the Linux kernel's SELinux subsystem in versions before 5.7. This flaw occurs while importing the Commercial IP Security Option (CIPSO) protocol's category bitmap into the SELinux extensible bitmap via the' ebitmap_netlbl_import' routine. While processing the CIPSO restricted bitmap tag in the 'cipso_v4_parsetag_rbm' routine, it sets the security attribute to indicate that the category bitmap is present, even if it has not been allocated. This issue leads to a NULL pointer dereference issue while importing the same category bitmap into SELinux. This flaw allows a remote network user to crash the system kernel, resulting in a denial of service.
CVE-2020-10713	A flaw was found in grub2, prior to version 2.06. An attacker may use the GRUB 2 flaw to hijack and tamper the GRUB verification process. This flaw also allows the bypass of Secure Boot protections. In order to load an untrusted or modified kernel, an attacker would first need to establish access to the system such as gaining physical access, obtain the ability to alter a pxe-boot network, or have remote access to a networked system with root access. With this access, an attacker could then craft a string to cause a buffer overflow by injecting a malicious payload that leads to arbitrary code execution within GRUB. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-10722	A vulnerability was found in DPDK versions 18.05 and above. A missing check for an integer overflow in vhost_user_set_log_base() could result in a smaller memory map than requested, possibly allowing memory corruption.
CVE-2020-10723	A memory corruption issue was found in DPDK versions 17.05 and above. This flaw is caused by an integer truncation on the index of a payload. Under certain circumstances, the index (a UInt) is copied and truncated into a uint16, which can lead to out of bound indexing and possible memory corruption.

CVE-2020-10724	A vulnerability was found in DPDK versions 18.11 and above. The vhost-crypto library code is missing validations for user-supplied values, potentially allowing an information leak through an out-of-bounds memory read.
CVE-2020-10725	A flaw was found in DPDK version 19.11 and above that allows a malicious guest to cause a segmentation fault of the vhost-user backend application running on the host, which could result in a loss of connectivity for the other guests running on that host. This is caused by a missing validity check of the descriptor address in the function `virtio_dev_rx_batch_packed()`.
CVE-2020-10726	A vulnerability was found in DPDK versions 19.11 and above. A malicious container that has direct access to the vhost-user socket can keep sending VHOST_USER_GET_INFLIGHT_FD messages, causing a resource leak (file descriptors and virtual memory), which may result in a denial of service.
CVE-2020-10730	A NULL pointer dereference, or possible use-after-free flaw was found in Samba AD LDAP server in versions before 4.10.17, before 4.11.11 and before 4.12.4. Although some versions of Samba shipped with Red Hat Enterprise Linux do not support Samba in AD mode, the affected code is shipped with the libldb package. This flaw allows an authenticated user to possibly trigger a use-after-free or NULL pointer dereference. The highest threat from this vulnerability is to system availability.
CVE-2020-10732	A flaw was found in the Linux kernel's implementation of Userspace core dumps. This flaw allows an attacker with a local account to crash a trivial program and exfiltrate private kernel data.
CVE-2020-10736	An authorization bypass vulnerability was found in Ceph versions 15.2.0 before 15.2.2, where the ceph-mon and ceph-mgr daemons do not properly restrict access, resulting in gaining access to unauthorized resources. This flaw allows an authenticated client to modify the configuration and possibly conduct further attacks.
CVE-2020-10745	A flaw was found in all Samba versions before 4.10.17, before 4.11.11 and before 4.12.4 in the way it processed NetBios over TCP/IP. This flaw allows a remote attacker could to cause the Samba server to consume excessive CPU use, resulting in a denial of service. This highest threat from this vulnerability is to system availability.
CVE-2020-10751	A flaw was found in the Linux kernels SELinux LSM hook implementation before version 5.7, where it incorrectly assumed that an skb would only contain a single netlink message. The hook would incorrectly only validate the first netlink message in the skb and allow

	or deny the rest of the messages within the skb with the granted permission without further processing.
CVE-2020-10753	A flaw was found in the Red Hat Ceph Storage RadosGW (Ceph Object Gateway). The vulnerability is related to the injection of HTTP headers via a CORS ExposeHeader tag. The newline character in the ExposeHeader tag in the CORS configuration file generates a header injection in the response when the CORS request is made. Ceph versions 3.x and 4.x are vulnerable to this issue.
CVE-2020-10755	An insecure-credentials flaw was found in all openstack-cinder versions before openstack-cinder 14.1.0, all openstack-cinder 15.x.x versions before openstack-cinder 15.2.0 and all openstack-cinder 16.x.x versions before openstack-cinder 16.1.0. When using openstack-cinder with the Dell EMC ScaleIO or VxFlex OS backend storage driver, credentials for the entire backend are exposed in the ``connection_info`` element in all Block Storage v3 Attachments API calls containing that element. This flaw enables an end-user to create a volume, make an API call to show the attachment detail information, and retrieve a username and password that may be used to connect to another user's volume. Additionally, these credentials are valid for the ScaleIO or VxFlex OS Management API, should an attacker discover the Management API endpoint. Source: OpenStack project
CVE-2020-10756	An out-of-bounds read vulnerability was found in the SLiRP networking implementation of the QEMU emulator. This flaw occurs in the icmp6_send_echoreply() routine while replying to an ICMP echo request, also known as ping. This flaw allows a malicious guest to leak the contents of the host memory, resulting in possible information disclosure. This flaw affects versions of libslirp before 4.3.1.
CVE-2020-10757	A flaw was found in the Linux Kernel in versions after 4.5-rc1 in the way mremap handled DAX Huge Pages. This flaw allows a local attacker with access to a DAX enabled storage to escalate their privileges on the system.
CVE-2020-10759	A PGP signature bypass flaw was found in fwupd (all versions), which could lead to the installation of unsigned firmware. As per upstream, a signature bypass is theoretically possible, but not practical because the Linux Vendor Firmware Service (LVFS) is either not implemented or enabled in versions of fwupd shipped with Red Hat Enterprise Linux 7 and 8. The highest threat from this vulnerability is to confidentiality and integrity.
CVE-2020-10760	A use-after-free flaw was found in all samba LDAP server versions before 4.10.17, before 4.11.11, before

	4.12.4 used in a AC DC configuration. A Samba LDAP user could use this flaw to crash samba.
CVE-2020-10761	An assertion failure issue was found in the Network Block Device(NBD) Server in all QEMU versions before QEMU 5.0.1. This flaw occurs when an nbd-client sends a spec-compliant request that is near the boundary of maximum permitted request length. A remote nbd-client could use this flaw to crash the qemu-nbd server resulting in a denial of service.
CVE-2020-10766	A logic bug flaw was found in Linux kernel before 5.8-rc1 in the implementation of SSBD. A bug in the logic handling allows an attacker with a local account to disable SSBD protection during a context switch when additional speculative execution mitigations are in place. This issue was introduced when the per task/process conditional STIPB switching was added on top of the existing SSBD switching. The highest threat from this vulnerability is to confidentiality.
CVE-2020-10767	A flaw was found in the Linux kernel before 5.8-rc1 in the implementation of the Enhanced IBPB (Indirect Branch Prediction Barrier). The IBPB mitigation will be disabled when STIBP is not available or when the Enhanced Indirect Branch Restricted Speculation (IBRS) is available. This flaw allows a local attacker to perform a Spectre V2 style attack when this configuration is active. The highest threat from this vulnerability is to confidentiality.
CVE-2020-10768	A flaw was found in the Linux Kernel before 5.8-rc1 in the prctl() function, where it can be used to enable indirect branch speculation after it has been disabled. This call incorrectly reports it as being 'force disabled' when it is not and opens the system to Spectre v2 attacks. The highest threat from this vulnerability is to confidentiality.
CVE-2020-10781	A flaw was found in the Linux Kernel before 5.8-rc6 in the ZRAM kernel module, where a user with a local account and the ability to read the /sys/class/zram-control/hot_add file can create ZRAM device nodes in the /dev/ directory. This read allocates kernel memory and is not accounted for a user that triggers the creation of that ZRAM device. With this vulnerability, continually reading the device may consume a large amount of system memory and cause the Out-of-Memory (OOM) killer to activate and terminate random userspace processes, possibly making the system inoperable.
CVE-2020-10878	Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection.

CVE-2020-10933	An issue was discovered in Ruby 2.5.x through 2.5.7, 2.6.x through 2.6.5, and 2.7.0. If a victim calls BasicSocket#read_nonblock(requested_size, buffer, exception: false), the method resizes the buffer to fit the requested size, but no data is copied. Thus, the buffer string provides the previous value of the heap. This may expose possibly sensitive data from the interpreter.
CVE-2020-10957	In Dovecot before 2.3.10.1, unauthenticated sending of malformed parameters to a NOOP command causes a NULL Pointer Dereference and crash in submission-login, submission, or lmtp.
CVE-2020-10958	In Dovecot before 2.3.10.1, a crafted SMTP/LMTP message triggers an unauthenticated use-after-free bug in submission-login, submission, or lmtp, and can lead to a crash under circumstances involving many newlines after a command.
CVE-2020-10967	In Dovecot before 2.3.10.1, remote unauthenticated attackers can crash the lmtp or submission process by sending mail with an empty localpart.
CVE-2020-10994	In libImaging/Jpeg2KDecode.c in Pillow before 7.1.0, there are multiple out-of-bounds reads via a crafted JP2 file.
CVE-2020-11022	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
CVE-2020-11023	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
CVE-2020-11042	In FreeRDP greater than 1.1 and before 2.0.0, there is an out-of-bounds read in update_read_icon_info. It allows reading a attacker-defined amount of client memory (32bit unsigned -> 4GB) to an intermediate buffer. This can be used to crash the client or store information for later retrieval. This has been patched in 2.0.0.
CVE-2020-11044	In FreeRDP greater than 1.2 and before 2.0.0, a double free in update_read_cache_bitmap_v3_order crashes the client application if corrupted data from a manipulated server is parsed. This has been patched in 2.0.0.
CVE-2020-11045	In FreeRDP after 1.0 and before 2.0.0, there is an out-of-bound read in in update_read_bitmap_data that

	allows client memory to be read to an image buffer. The result displayed on screen as colour.
CVE-2020-11046	In FreeRDP after 1.0 and before 2.0.0, there is a stream out-of-bounds seek in update_read_synchronize that could lead to a later out-of-bounds read.
CVE-2020-11047	In FreeRDP after 1.1 and before 2.0.0, there is an out-of-bounds read in autodetect_recv_bandwidth_measure_results. A malicious server can extract up to 8 bytes of client memory with a manipulated message by providing a short input and reading the measurement result data. This has been patched in 2.0.0.
CVE-2020-11048	In FreeRDP after 1.0 and before 2.0.0, there is an out-of-bounds read. It only allows to abort a session. No data extraction is possible. This has been fixed in 2.0.0.
CVE-2020-11049	In FreeRDP after 1.1 and before 2.0.0, there is an out-of-bound read of client memory that is then passed on to the protocol parser. This has been patched in 2.0.0.
CVE-2020-11058	In FreeRDP after 1.1 and before 2.0.0, a stream out-of-bounds seek in rdp_read_font_capability_set could lead to a later out-of-bounds read. As a result, a manipulated client or server might force a disconnect due to an invalid data read. This has been fixed in 2.0.0.
CVE-2020-11095	In FreeRDP before version 2.1.2, an out of bound reads occurs resulting in accessing a memory location that is outside of the boundaries of the static array PRIMARY_DRAWING_ORDER_FIELD_BYTES. This is fixed in version 2.1.2.
CVE-2020-11096	In FreeRDP before version 2.1.2, there is a global OOB read in update_read_cache_bitmap_v3_order. As a workaround, one can disable bitmap cache with -bitmap-cache (default). This is fixed in version 2.1.2.
CVE-2020-11097	In FreeRDP before version 2.1.2, an out of bounds read occurs resulting in accessing a memory location that is outside of the boundaries of the static array PRIMARY_DRAWING_ORDER_FIELD_BYTES. This is fixed in version 2.1.2.
CVE-2020-11098	In FreeRDP before version 2.1.2, there is an out-of-bound read in glyph_cache_put. This affects all FreeRDP clients with `+glyph-cache` option enabled This is fixed in version 2.1.2.
CVE-2020-11099	In FreeRDP before version 2.1.2, there is an out of bounds read in license_read_new_or_upgrade_license_packet. A manipulated license packet can lead to out of bound reads to an internal buffer. This is fixed in version 2.1.2.
CVE-2020-11521	libfreerdp/codec/planar.c in FreeRDP version > 1.0 through 2.0.0-rc4 has an Out-of-bounds Write.

CVE-2020-11522	libfreerdp/gdi/gdi.c in FreeRDP > 1.0 through 2.0.0-rc4 has an Out-of-bounds Read.
CVE-2020-11523	libfreerdp/gdi/region.c in FreeRDP versions > 1.0 through 2.0.0-rc4 has an Integer Overflow.
CVE-2020-11524	libfreerdp/codec/interleaved.c in FreeRDP versions > 1.0 through 2.0.0-rc4 has an Out-of-bounds Write.
CVE-2020-11525	libfreerdp/cache/bitmap.c in FreeRDP versions > 1.0 through 2.0.0-rc4 has an Out of bounds read.
CVE-2020-11526	libfreerdp/core/update.c in FreeRDP versions > 1.1 through 2.0.0-rc4 has an Out-of-bounds Read.
CVE-2020-11538	In libImaging/SgiRleDecode.c in Pillow through 7.0.0, a number of out-of-bounds reads exist in the parsing of SGI image files, a different issue than CVE-2020-5311.
CVE-2020-11565	** DISPUTED ** An issue was discovered in the Linux kernel through 5.6.2. mpol_parse_str in mm/mempolicy.c has a stack-based out-of-bounds write because an empty nodelist is mishandled during mount option parsing, aka CID-aa9f7d5172fa. NOTE: Someone in the security community disagrees that this is a vulnerability because the issue “is a bug in parsing mount options which can only be specified by a privileged user, so triggering the bug does not grant any powers not already held.”.
CVE-2020-11651	An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class does not properly validate method calls. This allows a remote user to access some methods without authentication. These methods can be used to retrieve user tokens from the salt master and/or run arbitrary commands on salt minions.
CVE-2020-11652	An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class allows access to some methods that improperly sanitize paths. These methods allow arbitrary directory access to authenticated users.
CVE-2020-11655	SQLite through 3.31.1 allows attackers to cause a denial of service (segmentation fault) via a malformed window-function query because the AggInfo object's initialization is mishandled.
CVE-2020-11728	An issue was discovered in DAViCal Andrew's Web Libraries (AWL) through 0.60. Session management does not use a sufficiently hard-to-guess session key. Anyone who can guess the microsecond time (and the incrementing session_id) can impersonate a session.
CVE-2020-11736	fr-archive-libarchive.c in GNOME file-roller through 3.36.1 allows Directory Traversal during extraction because it lacks a check of whether a file's parent is a symlink to a directory outside of the intended extraction location.

CVE-2020-11758	An issue was discovered in OpenEXR before 2.4.1. There is an out-of-bounds read in ImfOptimizedPixelReading.h.
CVE-2020-11759	An issue was discovered in OpenEXR before 2.4.1. Because of integer overflows in CompositeDeepScanLine::Data::handleDeepFrameBuffer and readSampleCountForLineBlock, an attacker can write to an out-of-bounds pointer.
CVE-2020-11760	An issue was discovered in OpenEXR before 2.4.1. There is an out-of-bounds read during RLE uncompression in rleUncompress in ImfRle.cpp.
CVE-2020-11761	An issue was discovered in OpenEXR before 2.4.1. There is an out-of-bounds read during Huffman uncompression, as demonstrated by FastHufDecoder::refill in ImfFastHuf.cpp.
CVE-2020-11762	An issue was discovered in OpenEXR before 2.4.1. There is an out-of-bounds read and write in DwaCompressor::uncompress in ImfDwaCompressor.cpp when handling the UNKNOWN compression case.
CVE-2020-11763	An issue was discovered in OpenEXR before 2.4.1. There is an std::vector out-of-bounds read and write, as demonstrated by ImfTileOffsets.cpp.
CVE-2020-11764	An issue was discovered in OpenEXR before 2.4.1. There is an out-of-bounds write in copyIntoFrameBuffer in ImfMisc.cpp.
CVE-2020-11765	An issue was discovered in OpenEXR before 2.4.1. There is an off-by-one error in use of the ImfXdr.h read function by DwaCompressor::Classifier::Classifier, leading to an out-of-bounds read.
CVE-2020-11869	An integer overflow was found in QEMU 4.0.1 through 4.2.0 in the way it implemented ATI VGA emulation. This flaw occurs in the ati_2d_blt() routine in hw/display/ati-2d.c while handling MMIO write operations through the ati_mm_write() callback. A malicious guest could abuse this flaw to crash the QEMU process, resulting in a denial of service.
CVE-2020-11884	In the Linux kernel 4.19 through 5.6.7 on the s390 platform, code execution may occur because of a race condition, as demonstrated by code in enable_sacf_uaccess in arch/s390/lib/uaccess.c that fails to protect against a concurrent page table upgrade, aka CID-3f777e19d171. A crash could also occur.
CVE-2020-11931	An Ubuntu-specific modification to Pulseaudio to provide security mediation for Snap-packaged applications was found to have a bypass of intended access restriction for snaps which plugs any of pulseaudio, audio-playback or audio-record via unloading the pulseaudio snap policy module.

	This issue affects: pulseaudio 1:8.0 versions prior to 1:8.0-0ubuntu3.12; 1:11.1 versions prior to 1:11.1-1ubuntu7.7; 1:13.0 versions prior to 1:13.0-1ubuntu1.2; 1:13.99.1 versions prior to 1:13.99.1-1ubuntu3.2;
CVE-2020-11933	cloud-init as managed by snapd on Ubuntu Core 16 and Ubuntu Core 18 devices was run without restrictions on every boot, which a physical attacker could exploit by crafting cloud-init user-data/meta-data via external media to perform arbitrary changes on the device to bypass intended security mechanisms such as full disk encryption. This issue did not affect traditional Ubuntu systems. Fixed in snapd version 2.45.2, revision 8539 and core version 2.45.2, revision 9659.
CVE-2020-11934	It was discovered that snapctl user-open allowed altering the $XDG_DATA_DIRS environment variable when calling the system xdg-open. OpenURL() in usersession/userd/launcher.go would alter $XDG_DATA_DIRS to append a path to a directory controlled by the calling snap. A malicious snap could exploit this to bypass intended access restrictions to control how the host system xdg-open script opens the URL and, for example, execute a script shipped with the snap without confinement. This issue did not affect Ubuntu Core systems. Fixed in snapd versions 2.45.1ubuntu0.2, 2.45.1+18.04.2 and 2.45.1+20.04.2.
CVE-2020-11935	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-11937	In whoopsie, parse_report() from whoopsie.c allows a local attacker to cause a denial of service via a crafted file. The DoS is caused by resource exhaustion due to a memory leak. Fixed in 0.2.52.5ubuntu0.5, 0.2.62ubuntu0.5 and 0.2.69ubuntu0.1.
CVE-2020-11945	An issue was discovered in Squid before 5.0.2. A remote attacker can replay a sniffed Digest Authentication nonce to gain access to resources that are otherwise forbidden. This occurs because the attacker can overflow the nonce reference counter (a short integer). Remote code execution may occur if the pooled token credentials are freed (instead of replayed as valid credentials).
CVE-2020-11947	iscsi_aio_ioctl_cb in block/iscsi.c in QEMU 4.1.0 has a heap-based buffer over-read that may disclose unrelated information from process memory to an attacker.
CVE-2020-11958	re2c 1.3 has a heap-based buffer overflow in Scanner::fill in parse/scanner.cc via a long lexeme.

CVE-2020-11984	Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE
CVE-2020-11989	Apache Shiro before 1.5.3, when using Apache Shiro with Spring dynamic controllers, a specially crafted request may cause an authentication bypass.
CVE-2020-11993	Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.
CVE-2020-11996	A specially crafted sequence of HTTP/2 requests sent to Apache Tomcat 10.0.0-M1 to 10.0.0-M5, 9.0.0.M1 to 9.0.35 and 8.5.0 to 8.5.55 could trigger high CPU usage for several seconds. If a sufficient number of such requests were made on concurrent HTTP/2 connections, the server could become unresponsive.
CVE-2020-12049	An issue was discovered in dbus >= 1.3.0 before 1.12.18. The DBusServer in libdbus, as used in dbus-daemon, leaks file descriptors when a message exceeds the per-message file descriptor limit. A local attacker with access to the D-Bus system bus or another system service's private AF_UNIX socket could use this to make the system service reach its file descriptor limit, denying service to subsequent D-Bus clients.
CVE-2020-12066	CServer::SendMsg in engine/server/server.cpp in Teeworlds 0.7.x before 0.7.5 allows remote attackers to shut down the server.
CVE-2020-12100	In Dovecot before 2.3.11.3, uncontrolled recursion in submission, lmtp, and lda allows remote attackers to cause a denial of service (resource consumption) via a crafted e-mail message with deeply nested MIME parts.
CVE-2020-12114	A pivot_root race condition in fs/namespace.c in the Linux kernel 4.4.x before 4.4.221, 4.9.x before 4.9.221, 4.14.x before 4.14.178, 4.19.x before 4.19.119, and 5.x before 5.3 allows local users to cause a denial of service (panic) by corrupting a mountpoint reference counter.
CVE-2020-12135	bson before 0.8 incorrectly uses int rather than size_t for many variables, parameters, and return values. In particular, the bson_ensure_space() parameter bytesNeeded could have an integer overflow via properly constructed bson input.
CVE-2020-12243	In filter.c in slapd in OpenLDAP before 2.4.50, LDAP search filters with nested boolean expressions can result in denial of service (daemon crash).

CVE-2020-12284	cbs_jpeg_split_fragment in libavcodec/cbs_jpeg.c in FFmpeg 4.1 and 4.2.2 has a heap-based buffer overflow during JPEG_MARKER_SOS handling because of a missing length check.
CVE-2020-12351	Improper input validation in BlueZ may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.
CVE-2020-12352	Improper access control in BlueZ may allow an unauthenticated user to potentially enable information disclosure via adjacent access.
CVE-2020-12387	A race condition when running shutdown code for Web Worker led to a use-after-free vulnerability. This resulted in a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0.
CVE-2020-12390	Incorrect origin serialization of URLs with IPv6 addresses could lead to incorrect security checks. This vulnerability affects Firefox < 76.
CVE-2020-12391	Documents formed using data: URLs in an OBJECT element failed to inherit the CSP of the creating context. This allowed the execution of scripts that should have been blocked, albeit with a unique opaque origin. This vulnerability affects Firefox < 76.
CVE-2020-12392	The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP POST data of a request, which can be controlled by the website. If a user used the 'Copy as cURL' feature and pasted the command into a terminal, it could have resulted in the disclosure of local files. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0.
CVE-2020-12394	A logic flaw in our location bar implementation could have allowed a local attacker to spoof the current location by selecting a different origin and removing focus from the input element. This vulnerability affects Firefox < 76.
CVE-2020-12395	Mozilla developers and community members reported memory safety bugs present in Firefox 75 and Firefox ESR 68.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0.
CVE-2020-12396	Mozilla developers and community members reported memory safety bugs present in Firefox 75. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 76.

CVE-2020-12397	By encoding Unicode whitespace characters within the From email header, an attacker can spoof the sender email address that Thunderbird displays. This vulnerability affects Thunderbird < 68.8.0.
CVE-2020-12398	If Thunderbird is configured to use STARTTLS for an IMAP server, and the server sends a PREAUTH response, then Thunderbird will continue with an unencrypted connection, causing email data to be sent without protection. This vulnerability affects Thunderbird < 68.9.0.
CVE-2020-12399	NSS has shown timing differences when performing DSA signatures, which was exploitable and could eventually leak private keys. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9.
CVE-2020-12400	When converting coordinates from projective to affine, the modular inversion was not performed in constant time, resulting in a possible timing-based side channel attack. This vulnerability affects Firefox < 80 and Firefox for Android < 80.
CVE-2020-12401	During ECDSA signature generation, padding applied in the nonce designed to ensure constant-time scalar multiplication was removed, resulting in variable-time execution dependent on secret data. This vulnerability affects Firefox < 80 and Firefox for Android < 80.
CVE-2020-12402	During RSA key generation, bignum implementations used a variation of the Binary Extended Euclidean Algorithm which entailed significantly input-dependent flow. This allowed an attacker able to perform electromagnetic-based side channel attacks to record traces leading to the recovery of the secret primes. *Note:* An unmodified Firefox browser does not generate RSA keys in normal operation and is not affected, but products built on top of it might. This vulnerability affects Firefox < 78.
CVE-2020-12405	When browsing a malicious page, a race condition in our SharedWorkerService could occur and lead to a potentially exploitable crash. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9.
CVE-2020-12406	Mozilla Developer Iain Ireland discovered a missing type check during unboxed objects removal, resulting in a crash. We presume that with enough effort that it could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9.
CVE-2020-12407	Mozilla Developer Nicolas Silva found that when using WebRender, Firefox would under certain conditions leak arbitrary GPU memory to the visible screen. The leaked memory content was visible to the user, but not

	observable from web content. This vulnerability affects Firefox < 77.
CVE-2020-12408	When browsing a document hosted on an IP address, an attacker could insert certain characters to flip domain and path information in the address bar. This vulnerability affects Firefox < 77.
CVE-2020-12409	When using certain blank characters in a URL, they where incorrectly rendered as spaces instead of an encoded URL. This vulnerability affects Firefox < 77.
CVE-2020-12410	Mozilla developers reported memory safety bugs present in Firefox 76 and Firefox ESR 68.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9.
CVE-2020-12411	Mozilla developers reported memory safety bugs present in Firefox 76. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 77.
CVE-2020-12415	When "%2F" was present in a manifest URL, Firefox's AppCache behavior may have become confused and allowed a manifest to be served from a subdirectory. This could cause the appcache to be used to service requests for the top level directory. This vulnerability affects Firefox < 78.
CVE-2020-12416	A VideoStreamEncoder may have been freed in a race condition with VideoBroadcaster::AddOrUpdateSink, resulting in a use-after-free, memory corruption, and a potentially exploitable crash. This vulnerability affects Firefox < 78.
CVE-2020-12417	Due to confusion about ValueTags on JavaScript Objects, an object may pass through the type barrier, resulting in memory corruption and a potentially exploitable crash. *Note: this issue only affects Firefox on ARM64 platforms.* This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.
CVE-2020-12418	Manipulating individual parts of a URL object could have caused an out-of-bounds read, leaking process memory to malicious JavaScript. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.
CVE-2020-12419	When processing callbacks that occurred during window flushing in the parent process, the associated window may die; causing a use-after-free condition. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects

	Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.
CVE-2020-12420	When trying to connect to a STUN server, a race condition could have caused a use-after-free of a pointer, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.
CVE-2020-12421	When performing add-on updates, certificate chains terminating in non-built-in-roots were rejected (even if they were legitimately added by an administrator.) This could have caused add-ons to become out-of-date silently without notification to the user. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.
CVE-2020-12422	In non-standard configurations, a JPEG image created by JavaScript could have caused an internal variable to overflow, resulting in an out of bounds write, memory corruption, and a potentially exploitable crash. This vulnerability affects Firefox < 78.
CVE-2020-12424	When constructing a permission prompt for WebRTC, a URI was supplied from the content process. This URI was untrusted, and could have been the URI of an origin that was previously granted permission; bypassing the prompt. This vulnerability affects Firefox < 78.
CVE-2020-12425	Due to confusion processing a hyphen character in Date.parse(), a one-byte out of bounds read could have occurred, leading to potential information disclosure. This vulnerability affects Firefox < 78.
CVE-2020-12426	Mozilla developers and community members reported memory safety bugs present in Firefox 77. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 78.
CVE-2020-12464	usb_sg_cancel in drivers/usb/core/message.c in the Linux kernel before 5.6.8 has a use-after-free because a transfer occurs without a reference, aka CID-056ad39ee925.
CVE-2020-12655	An issue was discovered in xfs_agf_verify in fs/xfs/libxfs/xfs_alloc.c in the Linux kernel through 5.6.10. Attackers may trigger a sync of excessive duration via an XFS v5 image with crafted metadata, aka CID-d0c7feaf8767.
CVE-2020-12656	** DISPUTED ** gss_mech_free in net/sunrpc/auth_gss/gss_mech_switch.c in the rpcsec_gss_krb5 implementation in the Linux kernel through 5.6.10 lacks certain domain_release calls, leading to a memory leak. Note: This was disputed with the assertion that the issue does not grant any access not already available.

	It is a problem that on unloading a specific kernel module some memory is leaked, but loading kernel modules is a privileged operation. A user could also write a kernel module to consume any amount of memory they like and load that replicating the effect of this bug.
CVE-2020-12657	An issue was discovered in the Linux kernel before 5.6.5. There is a use-after-free in block/bfq-iosched.c related to bfq_idle_slice_timer_body.
CVE-2020-12659	An issue was discovered in the Linux kernel before 5.6.7. xdp_umem_reg in net/xdp/xdp_umem.c has an out-of-bounds write (by a user with the CAP_NET_ADMIN capability) because of a lack of headroom validation.
CVE-2020-12662	Unbound before 1.10.1 has Insufficient Control of Network Message Volume, aka an "NXNSAttack" issue. This is triggered by random subdomains in the NSDNAME in NS records.
CVE-2020-12663	Unbound before 1.10.1 has an infinite loop via malformed DNS answers received from upstream servers.
CVE-2020-12673	In Dovecot before 2.3.11.3, sending a specially formatted NTLM request will crash the auth service because of an out-of-bounds read.
CVE-2020-12674	In Dovecot before 2.3.11.3, sending a specially formatted RPA request will crash the auth service because a length of zero is mishandled.
CVE-2020-12695	The Open Connectivity Foundation UPnP specification before 2020-04-17 does not forbid the acceptance of a subscription request with a delivery URL on a different network segment than the fully qualified event-subscription URL, aka the CallStranger issue.
CVE-2020-12723	regcomp.c in Perl before 5.30.3 allows a buffer overflow via a crafted regular expression because of recursive S_study_chunk calls.
CVE-2020-12762	json-c through 0.14 has an integer overflow and out-of-bounds write via a large JSON file, as demonstrated by printbuf_memappend.
CVE-2020-12767	exif_entry_get_value in exif-entry.c in libexif 0.6.21 has a divide-by-zero error.
CVE-2020-12768	** DISPUTED ** An issue was discovered in the Linux kernel before 5.6. svm_cpu_uninit in arch/x86/kvm/svm.c has a memory leak, aka CID-d80b64ff297e. NOTE: third parties dispute this issue because it's a one-time leak at the boot, the size is negligible, and it can't be triggered at will.
CVE-2020-12770	An issue was discovered in the Linux kernel through 5.6.11. sg_write lacks an sg_remove_request call in a certain failure case, aka CID-83c6f2390040.

CVE-2020-12771	An issue was discovered in the Linux kernel through 5.6.11. btree_gc_coalesce in drivers/md/bcache/btree.c has a deadlock if a coalescing operation fails.
CVE-2020-12783	Exim through 4.93 has an out-of-bounds read in the SPA authenticator that could result in SPA/NTLM authentication bypass in auths/spa.c and auths/auth-spa.c.
CVE-2020-12826	A signal access-control issue was discovered in the Linux kernel before 5.6.5, aka CID-7395ea4e65c2. Because exec_id in include/linux/sched.h is only 32 bits, an integer overflow can interfere with a do_notify_parent protection mechanism. A child process can send an arbitrary signal to a parent process in a different security domain. Exploitation limitations include the amount of elapsed time before an integer overflow occurs, and the lack of scenarios where signals to a parent process present a substantial operational threat.
CVE-2020-12829	In QEMU through 5.0.0, an integer overflow was found in the SM501 display driver implementation. This flaw occurs in the COPY_AREA macro while handling MMIO write operations through the sm501_2d_engine_write() callback. A local attacker could abuse this flaw to crash the QEMU process in sm501_2d_operation() in hw/display/sm501.c on the host, resulting in a denial of service.
CVE-2020-12861	A heap buffer overflow in SANE Backends before 1.0.30 allows a malicious device connected to the same local network as the victim to execute arbitrary code, aka GHSL-2020-080.
CVE-2020-12862	An out-of-bounds read in SANE Backends before 1.0.30 may allow a malicious device connected to the same local network as the victim to read important information, such as the ASLR offsets of the program, aka GHSL-2020-082.
CVE-2020-12863	An out-of-bounds read in SANE Backends before 1.0.30 may allow a malicious device connected to the same local network as the victim to read important information, such as the ASLR offsets of the program, aka GHSL-2020-083.
CVE-2020-12864	An out-of-bounds read in SANE Backends before 1.0.30 may allow a malicious device connected to the same local network as the victim to read important information, such as the ASLR offsets of the program, aka GHSL-2020-081.
CVE-2020-12865	A heap buffer overflow in SANE Backends before 1.0.30 may allow a malicious device connected to the same local network as the victim to execute arbitrary code, aka GHSL-2020-084.

CVE-2020-12866	A NULL pointer dereference in SANE Backends before 1.0.30 allows a malicious device connected to the same local network as the victim to cause a denial of service, GHSL-2020-079.
CVE-2020-12867	A NULL pointer dereference in sanei_epson_net_read in SANE Backends before 1.0.30 allows a malicious device connected to the same local network as the victim to cause a denial of service, aka GHSL-2020-075.
CVE-2020-12888	The VFIO PCI driver in the Linux kernel through 5.6.13 mishandles attempts to access disabled memory space.
CVE-2020-13112	An issue was discovered in libexif before 0.6.22. Several buffer over-reads in EXIF MakerNote handling could lead to information disclosure and crashes. This is different from CVE-2020-0093.
CVE-2020-13113	An issue was discovered in libexif before 0.6.22. Use of uninitialized memory in EXIF Makernote handling could lead to crashes and potential use-after-free conditions.
CVE-2020-13114	An issue was discovered in libexif before 0.6.22. An unrestricted size in handling Canon EXIF MakerNote data could lead to consumption of large amounts of compute time for decoding EXIF data.
CVE-2020-13143	gadget_dev_desc_UDC_store in drivers/usb/gadget/configfs.c in the Linux kernel 3.16 through 5.6.13 relies on kstrdup without considering the possibility of an internal '\0' value, which allows attackers to trigger an out-of-bounds read, aka CID-15753588bcd4.
CVE-2020-13249	libmariadb/mariadb_lib.c in MariaDB Connector/C before 3.1.8 does not properly validate the content of an OK packet received from a server. NOTE: although mariadb_lib.c was originally based on code shipped for MySQL, this issue does not affect any MySQL components supported by Oracle.
CVE-2020-13253	sd_wp_addr in hw/sd/sd.c in QEMU 4.2.0 uses an unvalidated address, which leads to an out-of-bounds read during sdhci_write() operations. A guest OS user can crash the QEMU process.
CVE-2020-13254	An issue was discovered in Django 2.2 before 2.2.13 and 3.0 before 3.0.7. In cases where a memcached backend does not perform key validation, passing malformed cache keys could result in a key collision, and potential data leakage.
CVE-2020-13361	In QEMU 5.0.0 and earlier, es1370_transfer_audio in hw/audio/es1370.c does not properly validate the frame count, which allows guest OS users to trigger an out-of-bounds access during an es1370_write() operation.
CVE-2020-13362	In QEMU 5.0.0 and earlier, megasas_lookup_frame in hw/scsi/megasas.c has an out-of-bounds read via a crafted reply_queue_head field from a guest OS user.

CVE-2020-13396	An issue was discovered in FreeRDP before 2.1.1. An out-of-bounds (OOB) read vulnerability has been detected in ntlm_read_ChallengeMessage in winpr/libwinpr/sspi/NTLM/ntlm_message.c.
CVE-2020-13397	An issue was discovered in FreeRDP before 2.1.1. An out-of-bounds (OOB) read vulnerability has been detected in security_fips_decrypt in libfreerdp/core/security.c due to an uninitialized value.
CVE-2020-13398	An issue was discovered in FreeRDP before 2.1.1. An out-of-bounds (OOB) write vulnerability has been detected in crypto_rsa_common in libfreerdp/crypto/crypto.c.
CVE-2020-13434	SQLite through 3.32.0 has an integer overflow in sqlite3_str_vappendf in printf.c.
CVE-2020-13435	SQLite through 3.32.0 has a segmentation fault in sqlite3ExprCodeTarget in expr.c.
CVE-2020-13558	A code execution vulnerability exists in the AudioSourceProviderGStreamer functionality of Webkit WebKitGTK 2.30.1. A specially crafted web page can lead to a use after free.
CVE-2020-13596	An issue was discovered in Django 2.2 before 2.2.13 and 3.0 before 3.0.7. Query parameters generated by the Django admin ForeignKeyRawIdWidget were not properly URL encoded, leading to a possibility of an XSS attack.
CVE-2020-13630	ext/fts3/fts3.c in SQLite before 3.32.0 has a use-after-free in fts3EvalNextRow, related to the snippet feature.
CVE-2020-13631	SQLite before 3.32.0 allows a virtual table to be renamed to the name of one of its shadow tables, related to alter.c and build.c.
CVE-2020-13632	ext/fts3/fts3_snippet.c in SQLite before 3.32.0 has a NULL pointer dereference via a crafted matchinfo() query.
CVE-2020-13645	In GNOME glib-networking through 2.64.2, the implementation of GTlsClientConnection skips hostname verification of the server's TLS certificate if the application fails to specify the expected server identity. This is in contrast to its intended documented behavior, to fail the certificate verification. Applications that fail to provide the server identity, including Balsa before 2.5.11 and 2.6.x before 2.6.1, accept a TLS certificate if the certificate is valid for any host.
CVE-2020-13659	address_space_map in exec.c in QEMU 4.2.0 can trigger a NULL pointer dereference related to BounceBuffer.
CVE-2020-13753	The bubblewrap sandbox of WebKitGTK and WPE WebKit, prior to 2.28.3, failed to properly block access to CLONE_NEWUSER and the TIOCSTI ioctl. CLONE_NEWUSER could potentially be used

	to confuse xdg-desktop-portal, which allows access outside the sandbox. TIOCSTI can be used to directly execute commands outside the sandbox by writing to the controlling terminal's input buffer, similar to CVE-2017-5226.
CVE-2020-13754	hw/pci/msix.c in QEMU 4.2.0 allows guest OS users to trigger an out-of-bounds access via a crafted address in an msi-x mmio operation.
CVE-2020-13777	GnuTLS 3.6.x before 3.6.14 uses incorrect cryptography for encrypting a session ticket (a loss of confidentiality in TLS 1.2, and an authentication bypass in TLS 1.3). The earliest affected version is 3.6.4 (2018-09-24) because of an error in a 2018-09-18 commit. Until the first key rotation, the TLS server always uses wrong data in place of an encryption key derived from an application.
CVE-2020-13790	libjpeg-turbo 2.0.4, and mozjpeg 4.0.0, has a heap-based buffer over-read in get_rgb_row() in rdppm.c via a malformed PPM input file.
CVE-2020-13800	ati-vga in hw/display/ati.c in QEMU 4.2.0 allows guest OS users to trigger infinite recursion via a crafted mm_index value during an ati_mm_read or ati_mm_write call.
CVE-2020-13881	In support.c in pam_tacplus 1.3.8 through 1.5.1, the TACACS+ shared secret gets logged via syslog if the DEBUG loglevel and journald are used.
CVE-2020-13904	FFmpeg 2.8 and 4.2.3 has a use-after-free via a crafted EXTINF duration in an m3u8 file because parse_playlist in libavformat/hls.c frees a pointer, and later that pointer is accessed in av_probe_input_format3 in libavformat/format.c.
CVE-2020-13934	An h2c direct connection to Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M5 to 9.0.36 and 8.5.1 to 8.5.56 did not release the HTTP/1.1 processor after the upgrade to HTTP/2. If a sufficient number of such requests were made, an OutOfMemoryException could occur leading to a denial of service.
CVE-2020-13935	The payload length in a WebSocket frame was not correctly validated in Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M1 to 9.0.36, 8.5.0 to 8.5.56 and 7.0.27 to 7.0.104. Invalid payload lengths could trigger an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service.
CVE-2020-13974	An issue was discovered in the Linux kernel 4.4 through 5.7.1. drivers/tty/vt/keyboard.c has an integer overflow if k_ascii is called several times in a row, aka CID-b86dab054059. NOTE: Members in the community argue that the integer overflow does not lead to a security issue in this case.

CVE-2020-14001	The kramdown gem before 2.3.0 for Ruby processes the template option inside Kramdown documents by default, which allows unintended read access (such as template="/etc/passwd") or unintended embedded Ruby code execution (such as a string that begins with template="string://<%= `). NOTE: kramdown is used in Jekyll, GitLab Pages, GitHub Pages, and Thredded Forum.
CVE-2020-14093	Mutt before 1.14.3 allows an IMAP fcc/postpone man-in-the-middle attack via a PREAUTH response.
CVE-2020-14145	The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client).
CVE-2020-14154	Mutt before 1.14.3 proceeds with a connection even if, in response to a GnuTLS certificate prompt, the user rejects an expired intermediate certificate.
CVE-2020-14303	A flaw was found in the AD DC NBT server in all Samba versions before 4.10.17, before 4.11.11 and before 4.12.4. A samba user could send an empty UDP packet to cause the samba server to crash.
CVE-2020-14308	In grub2 versions before 2.06 the grub memory allocator doesn't check for possible arithmetic overflows on the requested allocation size. This leads the function to return invalid memory allocations which can be further used to cause possible integrity, confidentiality and availability impacts during the boot process.
CVE-2020-14309	There's an issue with grub2 in all versions before 2.06 when handling squashfs filesystems containing a symbolic link with name length of UINT32 bytes in size. The name size leads to an arithmetic overflow leading to a zero-size allocation further causing a heap-based buffer overflow with attacker controlled data.
CVE-2020-14310	There is an issue on grub2 before version 2.06 at function read_section_as_string(). It expects a font name to be at max UINT32_MAX - 1 length in bytes but it doesn't verify it before proceed with buffer allocation to read the value from the font value. An attacker may leverage that by crafting a malicious font file which has a name with UINT32_MAX, leading to read_section_as_string() to an arithmetic overflow, zero-sized allocation and further heap-based buffer overflow.
CVE-2020-14311	There is an issue with grub2 before version 2.06 while handling symlink on ext filesystems. A filesystem containing a symbolic link with an inode size of UINT32_MAX causes an arithmetic overflow leading to

	a zero-sized memory allocation with subsequent heap-based buffer overflow.
CVE-2020-14314	A memory out-of-bounds read flaw was found in the Linux kernel before 5.9-rc2 with the ext3/ext4 file system, in the way it accesses a directory with broken indexing. This flaw allows a local user to crash the system if the directory exists. The highest threat from this vulnerability is to system availability.
CVE-2020-14318	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.
CVE-2020-14323	A null pointer dereference flaw was found in samba's Winbind service in versions before 4.11.15, before 4.12.9 and before 4.13.1. A local user could use this flaw to crash the winbind service causing denial of service.
CVE-2020-14344	An integer overflow leading to a heap-buffer overflow was found in The X Input Method (XIM) client was implemented in libX11 before version 1.6.10. As per upstream this is security relevant when setuid programs call XIM client functions while running with elevated privileges. No such programs are shipped with Red Hat Enterprise Linux.
CVE-2020-14345	A flaw was found in X.Org Server before xorg-x11-server 1.20.9. An Out-Of-Bounds access in XkbSetNames function may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14346	A flaw was found in xorg-x11-server before 1.20.9. An integer underflow in the X input extension protocol decoding in the X server may lead to arbitrary access of memory contents. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14347	A flaw was found in the way xserver memory was not properly initialized. This could leak parts of server memory to the X client. In cases where Xorg server runs with elevated privileges, this could result in possible ASLR bypass. Xorg-server before version 1.20.9 is vulnerable.
CVE-2020-14349	It was found that PostgreSQL versions before 12.4, before 11.9 and before 10.14 did not properly sanitize the search_path during logical replication. An authenticated attacker could use this flaw in an attack similar to CVE-2018-1058, in order to execute arbitrary SQL command in the context of the user used for replication.

CVE-2020-14350	It was found that some PostgreSQL extensions did not use search_path safely in their installation script. An attacker with sufficient privileges could use this flaw to trick an administrator into executing a specially crafted script, during the installation or update of such extension. This affects PostgreSQL versions before 12.4, before 11.9, before 10.14, before 9.6.19, and before 9.5.23.
CVE-2020-14351	A flaw was found in the Linux kernel. A use-after-free memory flaw was found in the perf subsystem allowing a local attacker with permission to monitor perf events to corrupt memory and possibly escalate privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14355	Multiple buffer overflow vulnerabilities were found in the QUIC image decoding process of the SPICE remote display system, before spice-0.14.2-1. Both the SPICE client (spice-gtk) and server are affected by these flaws. These flaws allow a malicious client or server to send specially crafted messages that, when processed by the QUIC image compression algorithm, result in a process crash or potential code execution.
CVE-2020-14356	A flaw null pointer dereference in the Linux kernel cgroupv2 subsystem in versions before 5.7.10 was found in the way when reboot the system. A local user could use this flaw to crash the system or escalate their privileges on the system.
CVE-2020-14360	A flaw was found in the X.Org Server before version 1.20.10. An out-of-bounds access in the XkbSetMap function may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14361	A flaw was found in X.Org Server before xorg-x11-server 1.20.9. An Integer underflow leading to heap-buffer overflow may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14362	A flaw was found in X.Org Server before xorg-x11-server 1.20.9. An Integer underflow leading to heap-buffer overflow may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14363	An integer overflow vulnerability leading to a double-free was found in libX11. This flaw allows a local privileged attacker to cause an application compiled with libX11 to crash, or in some cases, result in arbitrary

	code execution. The highest threat from this flaw is to confidentiality, integrity as well as system availability.
CVE-2020-14364	An out-of-bounds read/write access flaw was found in the USB emulator of the QEMU in versions before 5.2.0. This issue occurs while processing USB packets from a guest when USBDevice 'setup_len' exceeds its 'data_buf[4096]' in the do_token_in, do_token_out routines. This flaw allows a guest user to crash the QEMU process, resulting in a denial of service, or the potential execution of arbitrary code with the privileges of the QEMU process on the host.
CVE-2020-14367	A flaw was found in chrony versions before 3.5.1 when creating the PID file under the /var/run/chrony folder. The file is created during chronyd startup while still running as the root user, and when it's opened for writing, chronyd does not check for an existing symbolic link with the same file name. This flaw allows an attacker with privileged access to create a symlink with the default PID file name pointing to any destination file in the system, resulting in data loss and a denial of service due to the path traversal.
CVE-2020-14374	A flaw was found in dpdk in versions before 18.11.10 and before 19.11.5. A flawed bounds checking in the copy_data function leads to a buffer overflow allowing an attacker in a virtual machine to write arbitrary data to any address in the vhost_crypto application. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14375	A flaw was found in dpdk in versions before 18.11.10 and before 19.11.5. Virtio ring descriptors, and the data they describe are in a region of memory accessible by from both the virtual machine and the host. An attacker in a VM can change the contents of the memory after vhost_crypto has validated it. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14376	A flaw was found in dpdk in versions before 18.11.10 and before 19.11.5. A lack of bounds checking when copying iv_data from the VM guest memory into host memory can lead to a large buffer overflow. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14377	A flaw was found in dpdk in versions before 18.11.10 and before 19.11.5. A complete lack of validation of attacker-controlled parameters can lead to a buffer over read. The results of the over read are then written back to the guest virtual machine memory. This vulnerability can be used by an attacker in a virtual machine to read significant amounts of host memory. The highest threat

	from this vulnerability is to data confidentiality and system availability.
CVE-2020-14378	An integer underflow in dpdk versions before 18.11.10 and before 19.11.5 in the `move_desc` function can lead to large amounts of CPU cycles being eaten up in a long running loop. An attacker could cause `move_desc` to get stuck in a 4,294,967,295-count iteration loop. Depending on how `vhost_crypto` is being used this could prevent other VMs or network tasks from being serviced by the busy DPDK lcore for an extended period.
CVE-2020-14382	A vulnerability was found in upstream release cryptsetup-2.2.0 where, there's a bug in LUKS2 format validation code, that is effectively invoked on every device/image presenting itself as LUKS2 container. The bug is in segments validation code in file 'lib/luks2/luks2_json_metadata.c' in function hdr_validate_segments(struct crypt_device *cd, json_object *hdr_jobj) where the code does not check for possible overflow on memory allocation used for intervals array (see statement "intervals = malloc(first_backup * sizeof(*intervals));"). Due to the bug, library can be *tricked* to expect such allocation was successful but for far less memory then originally expected. Later it may read data FROM image crafted by an attacker and actually write such data BEYOND allocated memory.
CVE-2020-14383	A flaw was found in samba's DNS server. An authenticated user could use this flaw to the RPC server to crash. This RPC server, which also serves protocols other than dnsserver, will be restarted after a short delay, but it is easy for an authenticated non administrative attacker to crash it again as soon as it returns. The Samba DNS server itself will continue to operate, but many RPC services will not.
CVE-2020-14385	A flaw was found in the Linux kernel before 5.9-rc4. A failure of the file system metadata validator in XFS can cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt. This can lead to the filesystem being shutdown, or otherwise rendered inaccessible until it is remounted, leading to a denial of service. The highest threat from this vulnerability is to system availability.
CVE-2020-14386	A flaw was found in the Linux kernel before 5.9-rc4. Memory corruption can be exploited to gain root privileges from unprivileged processes. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2020-14390	A flaw was found in the Linux kernel in versions before 5.9-rc6. When changing screen size, an out-of-bounds memory write can occur leading to memory corruption

	or a denial of service. Due to the nature of the flaw, privilege escalation cannot be fully ruled out.
CVE-2020-14396	An issue was discovered in LibVNCServer before 0.9.13. libvncclient/tls_openssl.c has a NULL pointer dereference.
CVE-2020-14397	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/rfbregion.c has a NULL pointer dereference.
CVE-2020-14398	An issue was discovered in LibVNCServer before 0.9.13. An improperly closed TCP connection causes an infinite loop in libvncclient/sockets.c.
CVE-2020-14399	** DISPUTED ** An issue was discovered in LibVNCServer before 0.9.13. Byte-aligned data is accessed through uint32_t pointers in libvncclient/rfbproto.c. NOTE: there is reportedly "no trust boundary crossed."
CVE-2020-14400	** DISPUTED ** An issue was discovered in LibVNCServer before 0.9.13. Byte-aligned data is accessed through uint16_t pointers in libvncserver/translate.c. NOTE: Third parties do not consider this to be a vulnerability as there is no known path of exploitation or cross of a trust boundary.
CVE-2020-14401	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/scale.c has a pixel_value integer overflow.
CVE-2020-14402	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/corre.c allows out-of-bounds access via encodings.
CVE-2020-14403	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/hextile.c allows out-of-bounds access via encodings.
CVE-2020-14404	An issue was discovered in LibVNCServer before 0.9.13. libvncserver/rre.c allows out-of-bounds access via encodings.
CVE-2020-14405	An issue was discovered in LibVNCServer before 0.9.13. libvncclient/rfbproto.c does not limit TextChat size.
CVE-2020-14415	oss_write in audio/ossaudio.c in QEMU before 5.0.0 mishandles a buffer position.
CVE-2020-14422	Lib/ipaddress.py in Python through 3.8.3 improperly computes hash values in the IPv4Interface and IPv6Interface classes, which might allow a remote attacker to cause a denial of service if an application is affected by the performance of a dictionary containing IPv4Interface or IPv6Interface objects, and this attacker can cause many dictionary entries to be created. This is fixed in: v3.5.10, v3.5.10rc1; v3.6.12; v3.7.9; v3.8.4, v3.8.4rc1, v3.8.5, v3.8.6, v3.8.6rc1; v3.9.0, v3.9.0b4, v3.9.0b5, v3.9.0rc1, v3.9.0rc2.

CVE-2020-14539	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.48 and prior, 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14540	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14547	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14550	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.48 and prior, 5.7.30 and prior and 8.0.20 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14553	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Pluggable Auth). Supported versions that are affected are 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network

	access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14556	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-14557	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well as unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N).
CVE-2020-14559	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 5.6.48 and prior, 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1

	Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-14562	Vulnerability in the Java SE product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 11.0.7 and 14.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14568	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14572	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2020-14573	Vulnerability in the Java SE product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 11.0.7 and 14.0.1. Difficult to

	exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14575	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14576	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: UDF). Supported versions that are affected are 5.7.30 and prior and 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14577	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as

	through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-14578	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14579	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14581	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through

	sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-14583	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2020-14586	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14588	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well

	as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N).
CVE-2020-14589	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14591	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Audit Plug-in). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14593	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.4 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N).

CVE-2020-14597	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14619	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14620	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14621	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).

CVE-2020-14622	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).
CVE-2020-14623	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14624	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: JSON). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14625	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14631	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Audit). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful

	attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14632	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Options). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14633	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14634	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 2.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-14636	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS

	Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2020-14637	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2020-14638	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2020-14639	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2020-14640	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Sample apps).

	Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2020-14641	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).
CVE-2020-14643	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2020-14644	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

CVE-2020-14645	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14651	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2020-14652	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-14654	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14656	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported

	versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14663	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14664	Vulnerability in the Java SE product of Oracle Java SE (component: JavaFX). The supported version that is affected is Java SE: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2020-14672	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability

	impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14678	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14680	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14687	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14697	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14702	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple

	protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-1472	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.
CVE-2020-14734	Vulnerability in the Oracle Text component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Oracle Text. Successful attacks of this vulnerability can result in takeover of Oracle Text. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14735	Vulnerability in the Scheduler component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Scheduler executes to compromise Scheduler. While the vulnerability is in Scheduler, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Scheduler. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).
CVE-2020-14736	Vulnerability in the Database Vault component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows high privileged attacker having Create Public Synonym privilege with network access via Oracle Net to compromise Database Vault. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Database Vault accessible data as well as unauthorized read access to a subset of Database Vault accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-14740	Vulnerability in the SQL Developer Install component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows low privileged

	attacker having Client Computer User Account privilege with logon to the infrastructure where SQL Developer Install executes to compromise SQL Developer Install. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of SQL Developer Install accessible data. CVSS 3.1 Base Score 2.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N).
CVE-2020-14741	Vulnerability in the Database Filesystem component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows high privileged attacker having Resource, Create Table, Create View, Create Procedure, Dbfs_role privilege with network access via Oracle Net to compromise Database Filesystem. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Database Filesystem. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14742	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having SYSDBA level account privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Core RDBMS accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14750	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14757	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). The supported version that is affected is 12.2.1.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the

	attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well as unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N).
CVE-2020-14760	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.31 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2020-14765	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14769	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14771	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can

	result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14773	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14775	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14776	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14777	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14779	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE:

	7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14781	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JNDI). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-14782	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS

	3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14785	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14786	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14789	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14790	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14791	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL

	Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.1 Base Score 2.2 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14792	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N).
CVE-2020-14793	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14794	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVE-2020-14796	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).
CVE-2020-14797	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14798	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some

	of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2020-14800	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Encryption). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14803	Vulnerability in the Java SE product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 11.0.8 and 15. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-14804	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: FTS). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVE-2020-14809	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14812	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14814	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14820	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2020-14821	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise

	MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14825	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14827	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31 and prior and 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.1 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).
CVE-2020-14828	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14829	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVE-2020-14830	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14836	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14837	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14838	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Privileges). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-14839	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a

	hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14841	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14844	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14845	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14846	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14848	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.21 and prior. Easily exploitable

	vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14852	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Charsets). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14853	Vulnerability in the MySQL Cluster product of Oracle MySQL (component: Cluster: NDBCluster Plugin). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Cluster. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Cluster accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Cluster. CVSS 3.1 Base Score 4.6 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L).
CVE-2020-14859	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14860	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: Roles). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL

	Server accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14861	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14866	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14867	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 5.6.49 and prior, 5.7.31 and prior and 8.0.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14868	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14869	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 5.7.31

	and prior and 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14870	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: X Plugin). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14873	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Logging). Supported versions that are affected are 8.0.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14878	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Security: LDAP Auth). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:A/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14882	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality,

	Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14883	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14888	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14891	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14893	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14901	Vulnerability in the RDBMS Security component of Oracle Database Server. The supported version that is affected is 19c. Easily exploitable vulnerability allows high privileged attacker having Analyze Any privilege with network access via Oracle Net to

	compromise RDBMS Security. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all RDBMS Security accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).
CVE-2020-14928	evolution-data-server (eds) through 3.36.3 has a STARTTLS buffering issue that affects SMTP and POP3. When a server sends a "begin TLS" response, eds reads additional data and evaluates it in a TLS context, aka "response injection."
CVE-2020-14954	Mutt before 1.14.4 and NeoMutt before 2020-06-19 have a STARTTLS buffering issue that affects IMAP, SMTP, and POP3. When a server sends a "begin TLS" response, the client reads additional data (e.g., from a man-in-the-middle attacker) and evaluates it in a TLS context, aka "response injection."
CVE-2020-15103	In FreeRDP less than or equal to 2.1.2, an integer overflow exists due to missing input sanitation in rdpegfx channel. All FreeRDP clients are affected. The input rectangles from the server are not checked against local surface coordinates and blindly accepted. A malicious server can send data that will crash the client later on (invalid length arguments to a `memcpy`) This has been fixed in 2.2.0. As a workaround, stop using command line arguments /gfx, /gfx-h264 and /network:auto
CVE-2020-15157	In containerd (an industry-standard container runtime) before version 1.2.14 there is a credential leaking vulnerability. If a container image manifest in the OCI Image format or Docker Image V2 Schema 2 format includes a URL for the location of a specific image layer (otherwise known as a “foreign layer”), the default containerd resolver will follow that URL to attempt to download it. In v1.2.x but not 1.3.0 or later, the default containerd resolver will provide its authentication credentials if the server where the URL is located presents an HTTP 401 status code along with registry-specific HTTP headers. If an attacker publishes a public image with a manifest that directs one of the layers to be fetched from a web server they control and they trick a user or system into pulling the image, they can obtain the credentials used for pulling that image. In some cases, this may be the user's username and password for the registry. In other cases, this may be the credentials attached to the cloud virtual instance which can grant access to other cloud resources in the account. The default containerd resolver is used by the cri-containerd plugin (which can be used by Kubernetes), the ctr development tool, and other client programs that have explicitly linked against it. This vulnerability has been fixed in containerd 1.2.14.

	containerd 1.3 and later are not affected. If you are using containerd 1.3 or later, you are not affected. If you are using cri-containerd in the 1.2 series or prior, you should ensure you only pull images from trusted sources. Other container runtimes built on top of containerd but not using the default resolver (such as Docker) are not affected.
CVE-2020-15180	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-15238	Blueman is a GTK+ Bluetooth Manager. In Blueman before 2.1.4, the DhcpClient method of the D-Bus interface to blueman-mechanism is prone to an argument injection vulnerability. The impact highly depends on the system configuration. If Polkit-1 is disabled and for versions lower than 2.0.6, any local user can possibly exploit this. If Polkit-1 is enabled for version 2.0.6 and later, a possible attacker needs to be allowed to use the `org.blueman.dhcp.client` action. That is limited to users in the wheel group in the shipped rules file that do have the privileges anyway. On systems with ISC DHCP client (dhclient), attackers can pass arguments to `ip link` with the interface name that can e.g. be used to bring down an interface or add an arbitrary XDP/BPF program. On systems with dhcpcd and without ISC DHCP client, attackers can even run arbitrary scripts by passing `-c/path/to/script` as an interface name. Patches are included in 2.1.4 and master that change the DhcpClient D-Bus method(s) to accept BlueZ network object paths instead of network interface names. A backport to 2.0(.8) is also available. As a workaround, make sure that Polkit-1-support is enabled and limit privileges for the `org.blueman.dhcp.client` action to users that are able to run arbitrary commands as root anyway in /usr/share/polkit-1/rules.d/blueman.rules.
CVE-2020-15250	In JUnit4 from version 4.7 and before 4.13.1, the test rule TemporaryFolder contains a local information disclosure vulnerability. On Unix like systems, the system's temporary directory is shared between all users on that system. Because of this, when files and directories are written into this directory they are, by default, readable by other users on that same system. This vulnerability does not allow other users to overwrite the contents of these directories or files. This is purely an information disclosure vulnerability. This vulnerability impacts you if the JUnit tests write sensitive information, like API keys or passwords, into the temporary folder, and the JUnit tests execute in an environment where the OS has other untrusted

	users. Because certain JDK file system APIs were only added in JDK 1.7, this this fix is dependent upon the version of the JDK you are using. For Java 1.7 and higher users: this vulnerability is fixed in 4.13.1. For Java 1.6 and lower users: no patch is available, you must use the workaround below. If you are unable to patch, or are stuck running on Java 1.6, specifying the `java.io.tmpdir` system environment variable to a directory that is exclusively owned by the executing user will fix this vulnerability. For more information, including an example of vulnerable code, see the referenced GitHub Security Advisory.
CVE-2020-15254	Crossbeam is a set of tools for concurrent programming. In crossbeam-channel before version 0.4.4, the bounded channel incorrectly assumes that `Vec::from_iter` has allocated capacity that same as the number of iterator elements. `Vec::from_iter` does not actually guarantee that and may allocate extra memory. The destructor of the `bounded` channel reconstructs `Vec` from the raw pointer based on the incorrect assumes described above. This is unsound and causing deallocation with the incorrect capacity when `Vec::from_iter` has allocated different sizes with the number of iterator elements. This has been fixed in crossbeam-channel 0.4.4.
CVE-2020-15257	containerd is an industry-standard container runtime and is available as a daemon for Linux and Windows. In containerd before versions 1.3.9 and 1.4.3, the containerd-shim API is improperly exposed to host network containers. Access controls for the shim’s API socket verified that the connecting process had an effective UID of 0, but did not otherwise restrict access to the abstract Unix domain socket. This would allow malicious containers running in the same network namespace as the shim, with an effective UID of 0 but otherwise reduced privileges, to cause new processes to be run with elevated privileges. This vulnerability has been fixed in containerd 1.3.9 and 1.4.3. Users should update to these versions as soon as they are released. It should be noted that containers started with an old version of containerd-shim should be stopped and restarted, as running containers will continue to be vulnerable even after an upgrade. If you are not providing the ability for untrusted users to start containers in the same network namespace as the shim (typically the "host" network namespace, for example with docker run --net=host or hostNetwork: true in a Kubernetes pod) and run with an effective UID of 0, you are not vulnerable to this issue. If you are running containers with a vulnerable configuration, you can deny access to all abstract sockets with AppArmor by adding a line similar to deny unix addr=@**, to

	your policy. It is best practice to run containers with a reduced set of privileges, with a non-zero UID, and with isolated namespaces. The containerd maintainers strongly advise against sharing namespaces with the host. Reducing the set of isolation mechanisms used for a container necessarily increases that container's privilege, regardless of what container runtime is used for running that container.
CVE-2020-15305	An issue was discovered in OpenEXR before 2.5.2. Invalid input could cause a use-after-free in DeepScanLineInputFile::DeepScanLineInputFile() in IlmImf/ImfDeepScanLineInputFile.cpp.
CVE-2020-15306	An issue was discovered in OpenEXR before v2.5.2. Invalid chunkCount attributes could cause a heap buffer overflow in getChunkOffsetTableSize() in IlmImf/ImfMisc.cpp.
CVE-2020-15358	In SQLite before 3.32.3, select.c mishandles query-flattener optimization, leading to a multiSelectOrderBy heap overflow because of misuse of transitive properties for constant propagation.
CVE-2020-15389	jp2/opj_decompress.c in OpenJPEG through 2.3.1 has a use-after-free that can be triggered if there is a mix of valid and invalid files in a directory operated on by the decompressor. Triggering a double-free may also be possible. This is related to calling opj_image_destroy twice.
CVE-2020-15393	In the Linux kernel 4.4 through 5.7.6, usbtest_disconnect in drivers/usb/misc/usbtest.c has a memory leak, aka CID-28ebeb8db770.
CVE-2020-15436	Use-after-free vulnerability in fs/block_dev.c in the Linux kernel before 5.8 allows local users to gain privileges or cause a denial of service by leveraging improper access to a certain error field.
CVE-2020-15437	The Linux kernel before version 5.8 is vulnerable to a NULL pointer dereference in drivers/tty/serial/8250/8250_core.c:serial8250_isa_init_ports() that allows local users to cause a denial of service by using the p->serial_in pointer which uninitialized.
CVE-2020-15570	The parse_report() function in whoopsie.c in Whoopsie through 0.2.69 mishandles memory allocation failures, which allows an attacker to cause a denial of service via a malformed crash file.
CVE-2020-15652	By observing the stack trace for JavaScript errors in web workers, it was possible to leak the result of a cross-origin redirect. This applied only to content that can be parsed as script. This vulnerability affects Firefox < 79, Firefox ESR < 68.11, Firefox ESR < 78.1, Thunderbird < 68.11, and Thunderbird < 78.1.

CVE-2020-15653	An iframe sandbox element with the allow-popups flag could be bypassed when using noopener links. This could have led to security issues for websites relying on sandbox configurations that allowed popups and hosted arbitrary content. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1.
CVE-2020-15654	When in an endless loop, a website specifying a custom cursor using CSS could make it look like the user is interacting with the user interface, when they are not. This could lead to a perceived broken state, especially when interactions with existing browser dialogs and warnings do not work. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1.
CVE-2020-15655	A redirected HTTP request which is observed or modified through a web extension could bypass existing CORS checks, leading to potential disclosure of cross-origin information. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1.
CVE-2020-15656	JIT optimizations involving the Javascript arguments object could confuse later optimizations. This risk was already mitigated by various precautions in the code, resulting in this bug rated at only moderate severity. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1.
CVE-2020-15658	The code for downloading files did not properly take care of special characters, which led to an attacker being able to cut off the file ending at an earlier position, leading to a different file type being downloaded than shown in the dialog. This vulnerability affects Firefox ESR < 78.1, Firefox < 79, and Thunderbird < 78.1.
CVE-2020-15659	Mozilla developers and community members reported memory safety bugs present in Firefox 78 and Firefox ESR 78.0. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 79, Firefox ESR < 68.11, Firefox ESR < 78.1, Thunderbird < 68.11, and Thunderbird < 78.1.
CVE-2020-15664	By holding a reference to the eval() function from an about:blank window, a malicious webpage could have gained access to the InstallTrigger object which would allow them to prompt the user to install an extension. Combined with user confusion, this could result in an unintended or malicious extension being installed. This vulnerability affects Firefox < 80, Thunderbird < 78.2, Thunderbird < 68.12, Firefox ESR < 68.12, Firefox ESR < 78.2, and Firefox for Android < 80.
CVE-2020-15665	Firefox did not reset the address bar after the beforeunload dialog was shown if the user chose to remain on the page. This could have resulted in an

	incorrect URL being shown when used in conjunction with other unexpected browser behaviors. This vulnerability affects Firefox < 80.
CVE-2020-15666	When trying to load a non-video in an audio/video context the exact status code (200, 302, 404, 500, 412, 403, etc.) was disclosed via the MediaError Message. This level of information leakage is inconsistent with the standardized onerror/onsuccess disclosure and can lead to inferring login status to services or device discovery on a local network among other attacks. This vulnerability affects Firefox < 80 and Firefox for Android < 80.
CVE-2020-15668	A lock was missing when accessing a data structure and importing certificate information into the trust database. This vulnerability affects Firefox < 80 and Firefox for Android < 80.
CVE-2020-15670	Mozilla developers reported memory safety bugs present in Firefox for Android 79. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 80, Firefox ESR < 78.2, Thunderbird < 78.2, and Firefox for Android < 80.
CVE-2020-15673	Mozilla developers reported memory safety bugs present in Firefox 80 and Firefox ESR 78.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3.
CVE-2020-15674	Mozilla developers reported memory safety bugs present in Firefox 80. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 81.
CVE-2020-15675	When processing surfaces, the lifetime may outlive a persistent buffer leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 81.
CVE-2020-15676	Firefox sometimes ran the onload handler for SVG elements that the DOM sanitizer decided to remove, resulting in JavaScript being executed after pasting attacker-controlled data into a contenteditable element. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3.
CVE-2020-15677	By exploiting an Open Redirect vulnerability on a website, an attacker could have spoofed the site displayed in the download file dialog to show the original site (the one suffering from the open redirect)

	rather than the site the file was actually downloaded from. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3.
CVE-2020-15678	When recursing through graphical layers while scrolling, an iterator may have become invalid, resulting in a potential use-after-free. This occurs because the function APZCTreeManager::ComputeClippedCompositionBounds did not follow iterator invalidation rules. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3.
CVE-2020-15680	If a valid external protocol handler was referenced in an image tag, the resulting broken image size could be distinguished from a broken image size of a non-existent protocol handler. This allowed an attacker to successfully probe whether an external protocol handler was registered. This vulnerability affects Firefox < 82.
CVE-2020-15681	When multiple WASM threads had a reference to a module, and were looking up exported functions, one WASM thread could have overwritten another's entry in a shared stub table, resulting in a potentially exploitable crash. This vulnerability affects Firefox < 82.
CVE-2020-15682	When a link to an external protocol was clicked, a prompt was presented that allowed the user to choose what application to open it in. An attacker could induce that prompt to be associated with an origin they didn't control, resulting in a spoofing attack. This was fixed by changing external protocol prompts to be tab-modal while also ensuring they could not be incorrectly associated with a different origin. This vulnerability affects Firefox < 82.
CVE-2020-15683	Mozilla developers and community members reported memory safety bugs present in Firefox 81 and Firefox ESR 78.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 78.4, Firefox < 82, and Thunderbird < 78.4.
CVE-2020-15684	Mozilla developers reported memory safety bugs present in Firefox 81. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 82.
CVE-2020-15701	An unhandled exception in check_ignored() in apport/report.py can be exploited by a local attacker to cause a denial of service. If the mtime attribute is a string value in apport-ignore.xml, it will trigger an unhandled exception, resulting in a crash.

	Fixed in 2.20.1-0ubuntu2.24, 2.20.9-0ubuntu7.16, 2.20.11-0ubuntu27.6.
CVE-2020-15702	TOCTOU Race Condition vulnerability in apport allows a local attacker to escalate privileges and execute arbitrary code. An attacker may exit the crashed process and exploit PID recycling to spawn a root process with the same PID as the crashed process, which can then be used to escalate privileges. Fixed in 2.20.1-0ubuntu2.24, 2.20.9 versions prior to 2.20.9-0ubuntu7.16 and 2.20.11 versions prior to 2.20.11-0ubuntu27.6. Was ZDI-CAN-11234.
CVE-2020-15703	There is no input validation on the Locale property in an apt transaction. An unprivileged user can supply a full path to a writable directory, which lets aptd read a file as root. Having a symlink in place results in an error message if the file exists, and no error otherwise. This way an unprivileged user can check for the existence of any files on the system as root.
CVE-2020-15704	The modprobe child process in the ./debian/patches/load_ppp_generic_if_needed patch file incorrectly handled module loading. A local non-root attacker could exploit the MODPROBE_OPTIONS environment variable to read arbitrary root files. Fixed in 2.4.5-5ubuntu1.4, 2.4.5-5.1ubuntu2.3+esm2, 2.4.7-1+2ubuntu1.16.04.3, 2.4.7-2+2ubuntu1.3, 2.4.7-2+4.1ubuntu5.1, 2.4.7-2+4.1ubuntu6. Was ZDI-CAN-11504.
CVE-2020-15705	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions.
CVE-2020-15706	GRUB2 contains a race condition in grub_script_function_create() leading to a use-after-free vulnerability which can be triggered by redefining a function whilst the same function is already executing, leading to arbitrary code execution and secure boot restriction bypass. This issue affects GRUB2 version 2.04 and prior versions.
CVE-2020-15707	Integer overflows were discovered in the functions grub_cmd_initrd and grub_initrd_init in the efilinux component of GRUB2, as shipped in Debian, Red Hat, and Ubuntu (the functionality is not included in GRUB2 upstream), leading to a heap-based buffer overflow. These could be triggered by an extremely large number of arguments to the initrd command on 32-bit architectures, or a crafted filesystem with very large files on any architecture. An attacker could use this to execute arbitrary code and bypass UEFI Secure

	Boot restrictions. This issue affects GRUB2 version 2.04 and prior versions.
CVE-2020-15708	Ubuntu's packaging of libvirt in 20.04 LTS created a control socket with world read and write permissions. An attacker could use this to overwrite arbitrary files or execute arbitrary code.
CVE-2020-15709	Versions of add-apt-repository before 0.98.9.2, 0.96.24.32.14, 0.96.20.10, and 0.92.37.8ubuntu0.1~esm1, printed a PPA (personal package archive) description to the terminal as-is, which allowed PPA owners to provide ANSI terminal escapes to modify terminal contents in unexpected ways.
CVE-2020-15780	An issue was discovered in drivers/acpi/acpi_configfs.c in the Linux kernel before 5.7.7. Injection of malicious ACPI tables via configfs could be used by attackers to bypass lockdown and secure boot restrictions, aka CID-75b0cea7bf30.
CVE-2020-15810	An issue was discovered in Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Smuggling attacks may succeed against HTTP and HTTPS traffic. This leads to cache poisoning. This allows any client, including browser scripts, to bypass local security and poison the proxy cache and any downstream caches with content from an arbitrary source. When configured for relaxed header parsing (the default), Squid relays headers containing whitespace characters to upstream servers. When this occurs as a prefix to a Content-Length header, the frame length specified will be ignored by Squid (allowing for a conflicting length to be used from another Content-Length header) but relayed upstream.
CVE-2020-15811	An issue was discovered in Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Splitting attacks may succeed against HTTP and HTTPS traffic. This leads to cache poisoning. This allows any client, including browser scripts, to bypass local security and poison the browser cache and any downstream caches with content from an arbitrary source. Squid uses a string search instead of parsing the Transfer-Encoding header to find chunked encoding. This allows an attacker to hide a second request inside Transfer-Encoding: it is interpreted by Squid as chunked and split out into a second request delivered upstream. Squid will then deliver two distinct responses to the client, corrupting any downstream caches.
CVE-2020-15859	QEMU 4.2.0 has a use-after-free in hw/net/e1000e_core.c because a guest OS user can trigger an e1000e packet with the data's address set to the e1000e's MMIO address.

CVE-2020-15861	Net-SNMP through 5.7.3 allows Escalation of Privileges because of UNIX symbolic link (symlink) following.
CVE-2020-15862	Net-SNMP through 5.7.3 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides the ability to run arbitrary commands as root.
CVE-2020-15863	hw/net/xgmac.c in the XGMAC Ethernet controller in QEMU before 07-20-2020 has a buffer overflow. This occurs during packet transmission and affects the highbank and midway emulated machines. A guest user or process could use this flaw to crash the QEMU process on the host, resulting in a denial of service or potential privileged code execution. This was fixed in commit 5519724a13664b43e225ca05351c60b4468e4555.
CVE-2020-15900	A memory corruption issue was found in Artifex Ghostscript 9.50 and 9.52. Use of a non-standard PostScript operator can allow overriding of file access controls. The 'rsearch' calculation for the 'post' size resulted in a size that was too large, and could underflow to max uint32_t. This was fixed in commit 5d499272b95a6b890a1397e11d20937de000d31b.
CVE-2020-15959	Insufficient policy enforcement in networking in Google Chrome prior to 85.0.4183.102 allowed an attacker who convinced the user to enable logging to obtain potentially sensitive information from process memory via social engineering.
CVE-2020-15960	Heap buffer overflow in storage in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2020-15961	Insufficient policy validation in extensions in Google Chrome prior to 85.0.4183.121 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2020-15962	Insufficient policy validation in serial in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2020-15963	Insufficient policy enforcement in extensions in Google Chrome prior to 85.0.4183.121 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2020-15964	Insufficient data validation in media in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2020-15965	Type confusion in V8 in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2020-15966	Insufficient policy enforcement in extensions in Google Chrome prior to 85.0.4183.121 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information via a crafted Chrome Extension.
CVE-2020-15967	Use after free in payments in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-15968	Use after free in Blink in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15969	Use after free in WebRTC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15970	Use after free in NFC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-15971	Use after free in printing in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-15972	Use after free in audio in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15973	Insufficient policy enforcement in extensions in Google Chrome prior to 86.0.4240.75 allowed an attacker who convinced a user to install a malicious extension to bypass same origin policy via a crafted Chrome Extension.
CVE-2020-15974	Integer overflow in Blink in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2020-15975	Integer overflow in SwiftShader in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15976	Use after free in WebXR in Google Chrome on Android prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15977	Insufficient data validation in dialogs in Google Chrome on OS X prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from disk via a crafted HTML page.

CVE-2020-15978	Insufficient data validation in navigation in Google Chrome on Android prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.
CVE-2020-15979	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15980	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 86.0.4240.75 allowed a local attacker to bypass navigation restrictions via crafted Intents.
CVE-2020-15981	Out of bounds read in audio in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-15982	Inappropriate implementation in cache in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-15983	Insufficient data validation in webUI in Google Chrome on ChromeOS prior to 86.0.4240.75 allowed a local attacker to bypass content security policy via a crafted HTML page.
CVE-2020-15984	Insufficient policy enforcement in Omnibox in Google Chrome on iOS prior to 86.0.4240.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted URL.
CVE-2020-15985	Inappropriate implementation in Blink in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-15986	Integer overflow in media in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15987	Use after free in WebRTC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted WebRTC stream.
CVE-2020-15988	Insufficient policy enforcement in downloads in Google Chrome on Windows prior to 86.0.4240.75 allowed a remote attacker who convinced the user to open files to execute arbitrary code via a crafted HTML page.
CVE-2020-15989	Uninitialized data in PDFium in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.
CVE-2020-15990	Use after free in autofill in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had

	compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-15991	Use after free in password manager in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-15992	Insufficient policy enforcement in networking in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page.
CVE-2020-15995	Out of bounds write in V8 in Google Chrome prior to 86.0.4240.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15999	Heap buffer overflow in Freetype in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16000	Inappropriate implementation in Blink in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16001	Use after free in media in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16002	Use after free in PDFium in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2020-16003	Use after free in printing in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16004	Use after free in user interface in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16005	Insufficient policy enforcement in ANGLE in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16006	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16007	Insufficient data validation in installer in Google Chrome prior to 86.0.4240.183 allowed a local attacker to potentially elevate privilege via a crafted filesystem.
CVE-2020-16008	Stack buffer overflow in WebRTC in Google Chrome prior to 86.0.4240.183 allowed a remote attacker

	to potentially exploit stack corruption via a crafted WebRTC packet.
CVE-2020-16009	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16012	Side-channel information leakage in graphics in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-16013	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.198 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16014	Use after free in PPAPI in Google Chrome prior to 87.0.4280.66 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-16015	Insufficient data validation in WASM in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16016	Inappropriate implementation in base in Google Chrome prior to 86.0.4240.193 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-16017	Use after free in site isolation in Google Chrome prior to 86.0.4240.198 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-16018	Use after free in payments in Google Chrome prior to 87.0.4280.66 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-16019	Inappropriate implementation in filesystem in Google Chrome on ChromeOS prior to 87.0.4280.66 allowed a remote attacker who had compromised the browser process to bypass noexec restrictions via a malicious file.
CVE-2020-16020	Inappropriate implementation in cryptohome in Google Chrome on ChromeOS prior to 87.0.4280.66 allowed a remote attacker who had compromised the browser process to bypass discretionary access control via a malicious file.
CVE-2020-16021	Race in image burner in Google Chrome on ChromeOS prior to 87.0.4280.66 allowed a remote attacker who had compromised the browser process to perform OS-level privilege escalation via a malicious file.

CVE-2020-16022	Insufficient policy enforcement in networking in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to potentially bypass firewall controls via a crafted HTML page.
CVE-2020-16023	Use after free in WebCodecs in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16024	Heap buffer overflow in UI in Google Chrome prior to 87.0.4280.66 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-16025	Heap buffer overflow in clipboard in Google Chrome prior to 87.0.4280.66 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-16026	Use after free in WebRTC in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16027	Insufficient policy enforcement in developer tools in Google Chrome prior to 87.0.4280.66 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from the user's disk via a crafted Chrome Extension.
CVE-2020-16028	Heap buffer overflow in WebRTC in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16029	Inappropriate implementation in PDFium in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to bypass navigation restrictions via a crafted PDF file.
CVE-2020-16030	Insufficient data validation in Blink in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2020-16031	Insufficient data validation in UI in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-16032	Insufficient data validation in sharing in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-16033	Inappropriate implementation in WebUSB in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-16034	Inappropriate implementation in WebRTC in Google Chrome prior to 87.0.4280.66 allowed a local attacker to bypass policy restrictions via a crafted HTML page.

CVE-2020-16035	Insufficient data validation in cros-disks in Google Chrome on ChromeOS prior to 87.0.4280.66 allowed a remote attacker who had compromised the browser process to bypass noexec restrictions via a malicious file.
CVE-2020-16036	Inappropriate implementation in cookies in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to bypass cookie restrictions via a crafted HTML page.
CVE-2020-16037	Use after free in clipboard in Google Chrome prior to 87.0.4280.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16038	Use after free in media in Google Chrome on OS X prior to 87.0.4280.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16039	Use after free in extensions in Google Chrome prior to 87.0.4280.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16040	Insufficient data validation in V8 in Google Chrome prior to 87.0.4280.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16041	Out of bounds read in networking in Google Chrome prior to 87.0.4280.88 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-16042	Uninitialized Use in V8 in Google Chrome prior to 87.0.4280.88 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-16043	Insufficient data validation in networking in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to bypass discretionary access control via malicious network traffic.
CVE-2020-16044	Use after free in WebRTC in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted SCTP packet.
CVE-2020-16092	In QEMU through 5.0.0, an assertion failure can occur in the network packet processing. This issue affects the e1000e and vmxnet3 network devices. A malicious guest user/process could use this flaw to abort the QEMU process on the host, resulting in a denial of service condition in net_tx_pkt_add_raw_fragment in hw/net/net_tx_pkt.c.
CVE-2020-16116	In kerfuffle/jobs.cpp in KDE Ark before 20.08.0, a crafted archive can install files outside the extraction directory via ../ directory traversal.
CVE-2020-16119	Use-after-free vulnerability in the Linux kernel exploitable by a local attacker due to reuse of a DCCP

	socket with an attached dccps_hc_tx_ccid object as a listener after being released. Fixed in Ubuntu Linux kernel 5.4.0-51.56, 5.3.0-68.63, 4.15.0-121.123, 4.4.0-193.224, 3.13.0.182.191 and 3.2.0-149.196.
CVE-2020-16120	Overlayfs did not properly perform permission checking when copying up files in an overlayfs and could be exploited from within a user namespace, if, for example, unprivileged user namespaces were allowed. It was possible to have a file not readable by an unprivileged user to be copied to a mountpoint controlled by the user, like a removable device. This was introduced in kernel version 4.19 by commit d1d04ef ("ovl: stack file ops"). This was fixed in kernel version 5.8 by commits 56230d9 ("ovl: verify permissions in ovl_path_open()"), 48bd024 ("ovl: switch to mounter creds in readdir") and 05acefb ("ovl: check permission to open real file"). Additionally, commits 130fdbc ("ovl: pass correct flags for opening real directory") and 292f902 ("ovl: call secutiry hook in ovl_real_ioctl()") in kernel 5.8 might also be desired or necessary. These additional commits introduced a regression in overlay mounts within user namespaces which prevented access to files with ownership outside of the user namespace. This regression was mitigated by subsequent commit b6650da ("ovl: do not fail because of O_NOATIMEi") in kernel 5.11.
CVE-2020-16121	PackageKit provided detailed error messages to unprivileged callers that exposed information about file presence and mimetype of files that the user would be unable to determine on its own.
CVE-2020-16122	PackageKit's apt backend mistakenly treated all local debs as trusted. The apt security model is based on repository trust and not on the contents of individual files. On sites with configured PolicyKit rules this may allow users to install malicious packages.
CVE-2020-16123	An Ubuntu-specific patch in PulseAudio created a race condition where the snap policy module would fail to identify a client connection from a snap as coming from a snap if SCM_CREDENTIALS were missing, allowing the snap to connect to PulseAudio without proper confinement. This could be exploited by an attacker to expose sensitive information. Fixed in 1:13.99.3-1ubuntu2, 1:13.99.2-1ubuntu2.1, 1:13.99.1-1ubuntu3.8, 1:11.1-1ubuntu7.11, and 1:8.0-0ubuntu3.15.
CVE-2020-16125	gdm3 versions before 3.36.2 or 3.38.2 would start gnome-initial-setup if gdm3 can't contact the accountservice service via dbus in a timely manner; on Ubuntu (and potentially derivatives) this could be be chained with an additional issue that could allow a local user to create a new privileged account.

CVE-2020-16126	An Ubuntu-specific modification to AccountsService in versions before 0.6.55-0ubuntu13.2, among other earlier versions, improperly dropped the ruid, allowing untrusted users to send signals to AccountService, thus stopping it from handling D-Bus messages in a timely fashion.
CVE-2020-16127	An Ubuntu-specific modification to AccountsService in versions before 0.6.55-0ubuntu13.2, among other earlier versions, would perform unbounded read operations on user-controlled ~/.pam_environment files, allowing an infinite loop if /dev/zero is symlinked to this location.
CVE-2020-16128	The aptdaemon DBus interface disclosed file existence disclosure by setting Terminal/DebconfSocket properties, aka GHSL-2020-192 and GHSL-2020-196. This affected versions prior to 1.1.1+bzr982-0ubuntu34.1, 1.1.1+bzr982-0ubuntu32.3, 1.1.1+bzr982-0ubuntu19.5, 1.1.1+bzr982-0ubuntu14.5.
CVE-2020-16135	libssh 0.9.4 has a NULL pointer dereference in tftpserver.c if ssh_buffer_new returns NULL.
CVE-2020-16166	The Linux kernel through 5.7.11 allows remote attackers to make observations that help to obtain sensitive information about the internal state of the network RNG, aka CID-f227e3ec3b5c. This is related to drivers/char/random.c and kernel/time/timer.c.
CVE-2020-16287	A buffer overflow vulnerability in lprn_is_black() in contrib/lips4/gdevlprn.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16288	A buffer overflow vulnerability in pj_common_print_page() in devices/gdevpjet.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16289	A buffer overflow vulnerability in cif_print_page() in devices/gdevcif.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16290	A buffer overflow vulnerability in jetp3852_print_page() in devices/gdev3852.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16291	A buffer overflow vulnerability in contrib/gdevdj9.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16292	A buffer overflow vulnerability in mj_raster_cmd() in contrib/japanese/gdevmjc.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a

	denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16293	A null pointer dereference vulnerability in compose_group_nonknockout_nonblend_isolated_allmask_common() in base/gxblend.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16294	A buffer overflow vulnerability in epsc_print_page() in devices/gdevepsc.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16295	A null pointer dereference vulnerability in clj_media_size() in devices/gdevclj.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16296	A buffer overflow vulnerability in GetNumWrongData() in contrib/lips4/gdevlips.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16297	A buffer overflow vulnerability in FloydSteinbergDitheringC() in contrib/gdevbjca.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16298	A buffer overflow vulnerability in mj_color_correct() in contrib/japanese/gdevmjc.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16299	A Division by Zero vulnerability in bj10v_print_page() in contrib/japanese/gdev10v.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16300	A buffer overflow vulnerability in tiff12_print_page() in devices/gdevtfnx.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16301	A buffer overflow vulnerability in okiibm_print_page1() in devices/gdevokii.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16302	A buffer overflow vulnerability in jetp3852_print_page() in devices/gdev3852.c of Artifex Software GhostScript v9.50 allows a remote attacker to escalate privileges via a crafted PDF file. This is fixed in v9.51.

CVE-2020-16303	A use-after-free vulnerability in xps_finish_image_path() in devices/vector/gdevxps.c of Artifex Software GhostScript v9.50 allows a remote attacker to escalate privileges via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16304	A buffer overflow vulnerability in image_render_color_thresh() in base/gxicolor.c of Artifex Software GhostScript v9.50 allows a remote attacker to escalate privileges via a crafted eps file. This is fixed in v9.51.
CVE-2020-16305	A buffer overflow vulnerability in pcx_write_rle() in contrib/japanese/gdev10v.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16306	A null pointer dereference vulnerability in devices/gdevtsep.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted postscript file. This is fixed in v9.51.
CVE-2020-16307	A null pointer dereference vulnerability in devices/vector/gdevtxtw.c and psi/zbfont.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted postscript file. This is fixed in v9.51.
CVE-2020-16308	A buffer overflow vulnerability in p_print_image() in devices/gdevcdj.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16309	A buffer overflow vulnerability in lxm5700m_print_page() in devices/gdevlxm.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted eps file. This is fixed in v9.51.
CVE-2020-16310	A division by zero vulnerability in dot24_print_page() in devices/gdevdm24.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-16587	A heap-based buffer overflow vulnerability exists in Academy Software Foundation OpenEXR 2.3.0 in chunkOffsetReconstruction in ImfMultiPartInputFile.cpp that can cause a denial of service via a crafted EXR file.
CVE-2020-16588	A Null Pointer Deference issue exists in Academy Software Foundation OpenEXR 2.3.0 in generatePreview in makePreview.cpp that can cause a denial of service via a crafted EXR file.
CVE-2020-16589	A head-based buffer overflow exists in Academy Software Foundation OpenEXR 2.3.0 in writeTileData in ImfTiledOutputFile.cpp that can cause a denial of service via a crafted EXR file.

CVE-2020-17380	A heap-based buffer overflow was found in QEMU through 5.0.0 in the SDHCI device emulation support. It could occur while doing a multi block SDMA transfer via the sdhci_sdma_transfer_multi_blocks() routine in hw/sd/sdhci.c. A guest user or process could use this flaw to crash the QEMU process on the host, resulting in a denial of service condition, or potentially execute arbitrary code with privileges of the QEMU process on the host.
CVE-2020-17489	An issue was discovered in certain configurations of GNOME gnome-shell through 3.36.4. When logging out of an account, the password box from the login dialog reappears with the password still visible. If the user had decided to have the password shown in cleartext at login time, it is then visible for a brief moment upon a logout. (If the password were never shown in cleartext, only the password length is revealed.)
CVE-2020-17538	A buffer overflow vulnerability in GetNumSameData() in contrib/lips4/gdevlips.c of Artifex Software GhostScript v9.50 allows a remote attacker to cause a denial of service via a crafted PDF file. This is fixed in v9.51.
CVE-2020-1927	In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an an unexpected URL within the request URL.
CVE-2020-1934	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.
CVE-2020-1957	Apache Shiro before 1.5.2, when using Apache Shiro with Spring dynamic controllers, a specially crafted request may cause an authentication bypass.
CVE-2020-1971	The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could

	trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).
CVE-2020-2099	Jenkins 2.213 and earlier, LTS 2.204.1 and earlier improperly reuses encryption key parameters in the Inbound TCP Agent Protocol/3, allowing unauthorized attackers with knowledge of agent names to obtain the connection secrets for those agents, which can be used to connect to Jenkins, impersonating those agents.
CVE-2020-2100	Jenkins 2.218 and earlier, LTS 2.204.1 and earlier was vulnerable to a UDP amplification reflection denial of service attack on port 33848.
CVE-2020-2101	Jenkins 2.218 and earlier, LTS 2.204.1 and earlier did not use a constant-time comparison function for validating connection secrets, which could potentially allow an attacker to use a timing attack to obtain this secret.
CVE-2020-2102	Jenkins 2.218 and earlier, LTS 2.204.1 and earlier used a non-constant time comparison function when validating an HMAC.
CVE-2020-2103	Jenkins 2.218 and earlier, LTS 2.204.1 and earlier exposed session identifiers on a user's detail object in the whoAmI diagnostic page.
CVE-2020-2104	Jenkins 2.218 and earlier, LTS 2.204.1 and earlier allowed users with Overall/Read access to view a JVM memory usage chart.
CVE-2020-2105	REST API endpoints in Jenkins 2.218 and earlier, LTS 2.204.1 and earlier were vulnerable to clickjacking attacks.
CVE-2020-2160	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier uses different representations of request URL paths, which allows attackers to craft URLs that allow bypassing CSRF protection of any target URL.

CVE-2020-2161	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier does not properly escape node labels that are shown in the form validation for label expressions on job configuration pages, resulting in a stored XSS vulnerability exploitable by users able to define node labels.
CVE-2020-2162	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier does not set Content-Security-Policy headers for files uploaded as file parameters to a build, resulting in a stored XSS vulnerability.
CVE-2020-2163	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier improperly processes HTML content of list view column headers, resulting in a stored XSS vulnerability exploitable by users able to control column headers.
CVE-2020-2220	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape the agent name in the build time trend page, resulting in a stored cross-site scripting vulnerability.
CVE-2020-2221	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape the upstream job's display name shown as part of a build cause, resulting in a stored cross-site scripting vulnerability.
CVE-2020-2222	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape the job name in the 'Keep this build forever' badge tooltip, resulting in a stored cross-site scripting vulnerability.
CVE-2020-2223	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape correctly the 'href' attribute of links to downstream jobs displayed in the build console page, resulting in a stored cross-site scripting vulnerability.
CVE-2020-2229	Jenkins 2.251 and earlier, LTS 2.235.3 and earlier does not escape the tooltip content of help icons, resulting in a stored cross-site scripting (XSS) vulnerability.
CVE-2020-2230	Jenkins 2.251 and earlier, LTS 2.235.3 and earlier does not escape the project naming strategy description, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by users with Overall/Manage permission.
CVE-2020-2231	Jenkins 2.251 and earlier, LTS 2.235.3 and earlier does not escape the remote address of the host starting a build via 'Trigger builds remotely', resulting in a stored cross-site scripting (XSS) vulnerability exploitable by users with Job/Configure permission or knowledge of the Authentication Token.
CVE-2020-24386	An issue was discovered in Dovecot before 2.3.13. By using IMAP IDLE, an authenticated attacker can trigger unhibernation via attacker-controlled parameters, leading to access to other users' email messages (and path disclosure).

CVE-2020-24394	In the Linux kernel before 5.7.8, fs/nfsd/vfs.c (in the NFS server) can set incorrect permissions on new filesystem objects when the filesystem lacks ACL support, aka CID-22cf8419f131. This occurs because the current umask is not considered.
CVE-2020-24490	Improper buffer restrictions in BlueZ may allow an unauthenticated user to potentially enable denial of service via adjacent access. This affects all Linux kernel versions that support BlueZ.
CVE-2020-24553	Go before 1.14.8 and 1.15.x before 1.15.1 allows XSS because text/html is the default for CGI/FCGI handlers that lack a Content-Type header.
CVE-2020-24583	An issue was discovered in Django 2.2 before 2.2.16, 3.0 before 3.0.10, and 3.1 before 3.1.1 (when Python 3.7+ is used). FILE_UPLOAD_DIRECTORY_PERMISSIONS mode was not applied to intermediate-level directories created in the process of uploading files. It was also not applied to intermediate-level collected static directories when using the collectstatic management command.
CVE-2020-24584	An issue was discovered in Django 2.2 before 2.2.16, 3.0 before 3.0.10, and 3.1 before 3.1.1 (when Python 3.7+ is used). The intermediate-level directories of the filesystem cache had the system's standard umask rather than 0o077.
CVE-2020-24606	Squid before 4.13 and 5.x before 5.0.4 allows a trusted peer to perform Denial of Service by consuming all available CPU cycles during handling of a crafted Cache Digest response message. This only occurs when cache_peer is used with the cache digests feature. The problem exists because peerDigestHandleReply() livelocking in peer_digest.cc mishandles EOF.
CVE-2020-24654	In KDE Ark before 20.08.1, a crafted TAR archive with symlinks can install files outside the extraction directory, as demonstrated by a write operation to a user's home directory.
CVE-2020-24659	An issue was discovered in GnuTLS before 3.6.15. A server can trigger a NULL pointer dereference in a TLS 1.3 client if a no_renegotiation alert is sent with unexpected timing, and then an invalid second handshake occurs. The crash happens in the application's error handling path, where the gnutls_deinit function is called after detecting a handshake failure.
CVE-2020-25084	QEMU 5.0.0 has a use-after-free in hw/usb/hcd-xhci.c because the usb_packet_map return value is not checked.
CVE-2020-25085	QEMU 5.0.0 has a heap-based Buffer Overflow in flatview_read_continue in exec.c because hw/sd/sdhci.c

	mishandles a write operation in the SDHC_BLKSIZE case.
CVE-2020-2510	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via OracleNet to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Core RDBMS. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).
CVE-2020-2511	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via OracleNet to compromise Core RDBMS. While the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Core RDBMS. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).
CVE-2020-2512	Vulnerability in the Database Gateway for ODBC component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via OracleNet to compromise Database Gateway for ODBC. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Database Gateway for ODBC. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2515	Vulnerability in the Database Gateway for ODBC component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via OracleNet to compromise Database Gateway for ODBC. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Database Gateway for ODBC accessible data as well as unauthorized read access to a subset of Database Gateway for ODBC accessible data and unauthorized ability to cause a partial denial of service (partial DOS)

	of Database Gateway for ODBC. CVSS 3.0 Base Score 5.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L).
CVE-2020-2516	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Materialized View, Create Table privilege with network access via OracleNet to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Core RDBMS accessible data. CVSS 3.0 Base Score 2.4 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N).
CVE-2020-2517	Vulnerability in the Database Gateway for ODBC component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, and 19c. Difficult to exploit vulnerability allows high privileged attacker having Create Procedure, Create Database Link privilege with network access via OracleNet to compromise Database Gateway for ODBC. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Database Gateway for ODBC accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Database Gateway for ODBC. CVSS 3.0 Base Score 3.3 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:L).
CVE-2020-2518	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-2519	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in

	unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.0 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L).
CVE-2020-25211	In the Linux kernel through 5.8.7, local attackers able to inject conntrack netlink configuration could overflow a local buffer, causing crashes or triggering use of incorrect protocol numbers in ctnetlink_parse_tuple_filter in net/netfilter/nf_conntrack_netlink.c, aka CID-1cc5ef91d2ff.
CVE-2020-25212	A TOCTOU mismatch in the NFS client code in the Linux kernel before 5.8.3 could be used by local attackers to corrupt memory or possibly have unspecified other impact because a size check is in fs/nfs/nfs4proc.c instead of fs/nfs/nfs4xdr.c, aka CID-b4487b935452.
CVE-2020-25219	url::recvline in url.cpp in libproxy 0.4.x through 0.4.15 allows a remote HTTP server to trigger uncontrolled recursion via a response composed of an infinite stream that lacks a newline character. This leads to stack exhaustion.
CVE-2020-2527	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Index, Create Table privilege with network access via OracleNet to compromise Core RDBMS. While the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Core RDBMS accessible data. CVSS 3.0 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).
CVE-2020-25275	Dovecot before 2.3.13 has Improper Input Validation in lda, lmtp, and imap, leading to an application crash via a crafted email message with certain choices for ten thousand MIME parts.
CVE-2020-25284	The rbd block device driver in drivers/block/rbd.c in the Linux kernel through 5.8.9 used incomplete permission checking for access to rbd devices, which could be leveraged by local attackers to map or unmap rbd block devices, aka CID-f44d04e696fe.
CVE-2020-25285	A race condition between hugetlb sysctl handlers in mm/hugetlb.c in the Linux kernel before 5.8.8 could be used by local attackers to corrupt memory, cause a NULL pointer dereference, or possibly have unspecified other impact, aka CID-17743798d812.
CVE-2020-2544	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console).

	Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2020-2546	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Application Container - JavaEE). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-2547	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N).
CVE-2020-2548	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: WLS Core Components). The supported version that is affected is 10.3.6.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server

	accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N).
CVE-2020-2549	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: WLS Core Components). The supported version that is affected is 10.3.6.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-2550	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where Oracle WebLogic Server executes to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data as well as unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:L/A:N).
CVE-2020-2551	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: WLS Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-2552	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: WLS Core Components). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products.

	Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:C/C:L/I:L/A:N).
CVE-2020-25613	An issue was discovered in Ruby through 2.5.8, 2.6.x through 2.6.6, and 2.7.x through 2.7.1. WEBrick, a simple HTTP server bundled with Ruby, had not checked the transfer-encoding header value rigorously. An attacker may potentially exploit this issue to bypass a reverse proxy (which also has a poor header check), which may lead to an HTTP Request Smuggling attack.
CVE-2020-25624	hw/usb/hcd-ohci.c in QEMU 5.0.0 has a stack-based buffer over-read via values obtained from the host controller driver.
CVE-2020-25625	hw/usb/hcd-ohci.c in QEMU 5.0.0 has an infinite loop when a TD list has a loop.
CVE-2020-25641	A flaw was found in the Linux kernel's implementation of biovecs in versions before 5.9-rc7. A zero-length biovec request issued by the block subsystem could cause the kernel to enter an infinite loop, causing a denial of service. This flaw allows a local attacker with basic privileges to issue requests to a block device, resulting in a denial of service. The highest threat from this vulnerability is to system availability.
CVE-2020-25643	A flaw was found in the HDLC_PPP module of the Linux kernel in versions before 5.9-rc7. Memory corruption and a read overflow is caused by improper input validation in the ppp_cp_parse_cr function which can cause the system to crash or cause a denial of service. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25645	A flaw was found in the Linux kernel in versions before 5.9-rc7. Traffic between two Geneve endpoints may be unencrypted when IPsec is configured to encrypt traffic for the specific UDP port used by the GENEVE tunnel allowing anyone between the two endpoints to read the traffic unencrypted. The main threat from this vulnerability is to data confidentiality.
CVE-2020-25650	A flaw was found in the way the spice-vdagentd daemon handled file transfers from the host system to the virtual machine. Any unprivileged local guest user with access to the UNIX domain socket path `/run/spice-vdagentd/spice-vdagent-sock` could use this flaw to perform a memory denial of service for spice-vdagentd or even other processes in the VM system. The highest threat from this vulnerability is to system

	availability. This flaw affects spice-vdagent versions 0.20 and previous versions.
CVE-2020-25651	A flaw was found in the SPICE file transfer protocol. File data from the host system can end up in full or in parts in the client connection of an illegitimate local user in the VM system. Active file transfers from other users could also be interrupted, resulting in a denial of service. The highest threat from this vulnerability is to data confidentiality as well as system availability. This flaw affects spice-vdagent versions 0.20 and prior.
CVE-2020-25652	A flaw was found in the spice-vdagentd daemon, where it did not properly handle client connections that can be established via the UNIX domain socket in `/run/spice-vdagentd/spice-vdagent-sock`. Any unprivileged local guest user could use this flaw to prevent legitimate agents from connecting to the spice-vdagentd daemon, resulting in a denial of service. The highest threat from this vulnerability is to system availability. This flaw affects spice-vdagent versions 0.20 and prior.
CVE-2020-25653	A race condition vulnerability was found in the way the spice-vdagentd daemon handled new client connections. This flaw may allow an unprivileged local guest user to become the active agent for spice-vdagentd, possibly resulting in a denial of service or information leakage from the host. The highest threat from this vulnerability is to data confidentiality as well as system availability. This flaw affects spice-vdagent versions 0.20 and prior.
CVE-2020-25654	An ACL bypass flaw was found in pacemaker. An attacker having a local account on the cluster and in the haclient group could use IPC communication with various daemons directly to perform certain tasks that they would be prevented by ACLs from doing if they went through the configuration.
CVE-2020-25656	A flaw was found in the Linux kernel. A use-after-free was found in the way the console subsystem was using ioctls KDGKBSENT and KDSKBSENT. A local user could use this flaw to get read memory access out of bounds. The highest threat from this vulnerability is to data confidentiality.
CVE-2020-25659	python-cryptography 3.2 is vulnerable to Bleichenbacher timing attacks in the RSA decryption API, via timed processing of valid PKCS#1 v1.5 ciphertext.
CVE-2020-25660	A flaw was found in the Cephx authentication protocol in versions before 15.2.6 and before 14.2.14, where it does not verify Ceph clients correctly and is then vulnerable to replay attacks in Nautilus. This flaw allows an attacker with access to the Ceph cluster network to authenticate with the Ceph service via a packet sniffer and perform actions allowed by the Ceph service. This

	issue is a reintroduction of CVE-2018-1128, affecting the msgr2 protocol. The msgr 2 protocol is used for all communication except older clients that do not support the msgr2 protocol. The msgr1 protocol is not affected. The highest threat from this vulnerability is to confidentiality, integrity, and system availability.
CVE-2020-25668	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-25669	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-2568	Vulnerability in the Oracle Applications DBA component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Oracle Applications DBA executes to compromise Oracle Applications DBA. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications DBA accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Applications DBA. CVSS 3.0 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L).
CVE-2020-25681	A flaw was found in dnsmasq before version 2.83. A heap-based buffer overflow was discovered in the way RRSets are sorted before validating with DNSSEC data. An attacker on the network, who can forge DNS replies such as that they are accepted as valid, could use this flaw to cause a buffer overflow with arbitrary data in a heap memory segment, possibly executing code on the machine. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25682	A flaw was found in dnsmasq before 2.83. A buffer overflow vulnerability was discovered in the way dnsmasq extract names from DNS packets before validating them with DNSSEC data. An attacker on the network, who can create valid DNS replies, could use this flaw to cause an overflow with arbitrary data in a heap-allocated memory, possibly executing code on the machine. The flaw is in the rfc1035.c:extract_name() function, which writes data to the memory pointed by

	name assuming MAXDNAME*2 bytes are available in the buffer. However, in some code execution paths, it is possible extract_name() gets passed an offset from the base buffer, thus reducing, in practice, the number of available bytes that can be written in the buffer. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25683	A flaw was found in dnsmasq before version 2.83. A heap-based buffer overflow was discovered in dnsmasq when DNSSEC is enabled and before it validates the received DNS entries. A remote attacker, who can create valid DNS replies, could use this flaw to cause an overflow in a heap-allocated memory. This flaw is caused by the lack of length checks in rfc1035.c:extract_name(), which could be abused to make the code execute memcpy() with a negative size in get_rdata() and cause a crash in dnsmasq, resulting in a denial of service. The highest threat from this vulnerability is to system availability.
CVE-2020-25684	A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in the forward.c:reply_query() if the reply destination address/port is used by the pending forwarded queries. However, it does not use the address/port to retrieve the exact forwarded query, substantially reducing the number of attempts an attacker on the network would have to perform to forge a reply and get it accepted by dnsmasq. This issue contrasts with RFC5452, which specifies a query's attributes that all must be used to match a reply. This flaw allows an attacker to perform a DNS Cache Poisoning attack. If chained with CVE-2020-25685 or CVE-2020-25686, the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.
CVE-2020-25685	A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in forward.c:reply_query(), which is the forwarded query that matches the reply, by only using a weak hash of the query name. Due to the weak hash (CRC32 when dnsmasq is compiled without DNSSEC, SHA-1 when it is) this flaw allows an off-path attacker to find several different domains all having the same hash, substantially reducing the number of attempts they would have to perform to forge a reply and get it accepted by dnsmasq. This is in contrast with RFC5452, which specifies that the query name is one of the attributes of a query that must be used to match a reply. This flaw could be abused to perform a DNS Cache Poisoning attack. If chained with CVE-2020-25684 the attack complexity of

	a successful attack is reduced. The highest threat from this vulnerability is to data integrity.
CVE-2020-25686	A flaw was found in dnsmasq before version 2.83. When receiving a query, dnsmasq does not check for an existing pending request for the same name and forwards a new request. By default, a maximum of 150 pending queries can be sent to upstream servers, so there can be at most 150 queries for the same name. This flaw allows an off-path attacker on the network to substantially reduce the number of attempts that it would have to perform to forge a reply and have it accepted by dnsmasq. This issue is mentioned in the "Birthday Attacks" section of RFC5452. If chained with CVE-2020-25684, the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.
CVE-2020-25687	A flaw was found in dnsmasq before version 2.83. A heap-based buffer overflow was discovered in dnsmasq when DNSSEC is enabled and before it validates the received DNS entries. This flaw allows a remote attacker, who can create valid DNS replies, to cause an overflow in a heap-allocated memory. This flaw is caused by the lack of length checks in rfc1035.c:extract_name(), which could be abused to make the code execute memcpy() with a negative size in sort_rrset() and cause a crash in dnsmasq, resulting in a denial of service. The highest threat from this vulnerability is to system availability.
CVE-2020-2569	Vulnerability in the Oracle Applications DBA component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Oracle Applications DBA executes to compromise Oracle Applications DBA. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications DBA accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Applications DBA. CVSS 3.0 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L).
CVE-2020-25692	A NULL pointer dereference was found in OpenLDAP server and was fixed in openldap 2.4.55, during a request for renaming RDNs. An unauthenticated attacker could remotely crash the slapd process by sending a specially crafted request, causing a Denial of Service.

CVE-2020-25694	A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. If a client application that creates additional database connections only reuses the basic connection parameters while dropping security-relevant parameters, an opportunity for a man-in-the-middle attack, or the ability to observe clear-text transmissions, could exist. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25695	A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. An attacker having permission to create non-temporary objects in at least one schema can execute arbitrary SQL functions under the identity of a superuser. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25696	A flaw was found in the psql interactive terminal of PostgreSQL in versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. If an interactive psql session uses \gset when querying a compromised server, the attacker can execute arbitrary code as the operating system account running psql. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25704	A flaw memory leak in the Linux kernel performance monitoring subsystem was found in the way if using PERF_EVENT_IOC_SET_FILTER. A local user could use this flaw to starve the resources causing denial of service.
CVE-2020-25705	A flaw in the way reply ICMP packets are limited in the Linux kernel functionality was found that allows to quickly scan open UDP ports. This flaw allows an off-path remote user to effectively bypassing source port UDP randomization. The highest threat from this vulnerability is to confidentiality and possibly integrity, because software that relies on UDP source port randomization are indirectly affected as well. Kernel versions before 5.10 may be vulnerable to this issue.
CVE-2020-25708	A divide by zero issue was found to occur in libvncserver-0.9.12. A malicious client could use this flaw to send a specially crafted message that, when processed by the VNC server, would lead to a floating point exception, resulting in a denial of service.
CVE-2020-25712	A flaw was found in xorg-x11-server before 1.20.10. A heap-buffer overflow in XkbSetDeviceInfo may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

CVE-2020-25723	A reachable assertion issue was found in the USB EHCI emulation code of QEMU. It could occur while processing USB requests due to missing handling of DMA memory map failure. A malicious privileged user within the guest may abuse this flaw to send bogus USB requests and crash the QEMU process on the host, resulting in a denial of service.
CVE-2020-2583	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2590	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-2593	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability

	allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-2601	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).
CVE-2020-2604	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE

	8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS v3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-26116	http.client in Python 3.x before 3.5.10, 3.6.x before 3.6.12, 3.7.x before 3.7.9, and 3.8.x before 3.8.5 allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of HTTPConnection.request.
CVE-2020-26137	urllib3 before 1.25.9 allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of putrequest(). NOTE: this is similar to CVE-2020-26116.
CVE-2020-26154	url.cpp in libproxy through 0.4.15 is prone to a buffer overflow when PAC is enabled, as demonstrated by a large PAC file that is delivered without a Content-length header.
CVE-2020-26217	XStream before version 1.4.14 is vulnerable to Remote Code Execution.The vulnerability may allow a remote attacker to run arbitrary shell commands only by manipulating the processed input stream. Only users who rely on blocklists are affected. Anyone using XStream's Security Framework allowlist is not affected. The linked advisory provides code workarounds for users who cannot upgrade. The issue is fixed in version 1.4.14.
CVE-2020-26258	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.15, a Server-Side Forgery Request vulnerability can be activated when unmarshalling. The vulnerability may allow a remote attacker to request data from internal resources that are not publicly available only by manipulating the processed input stream. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.15. The reported vulnerability does not exist if running Java 15 or higher. No user is affected who followed the recommendation to setup XStream's Security Framework with a whitelist! Anyone relying on XStream's default blacklist can immediately switch to a whilelist for the allowed types to avoid the vulnerability. Users of XStream 1.4.14 or below who still want to use XStream default blacklist can use a workaround described in more detailed in the referenced advisories.

CVE-2020-26259	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.15, is vulnerable to an Arbitrary File Deletion on the local host when unmarshalling. The vulnerability may allow a remote attacker to delete arbitrary know files on the host as log as the executing process has sufficient rights only by manipulating the processed input stream. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.15. The reported vulnerability does not exist running Java 15 or higher. No user is affected, who followed the recommendation to setup XStream's Security Framework with a whitelist! Anyone relying on XStream's default blacklist can immediately switch to a whilelist for the allowed types to avoid the vulnerability. Users of XStream 1.4.14 or below who still want to use XStream default blacklist can use a workaround described in more detailed in the referenced advisories.
CVE-2020-26262	Coturn is free open source implementation of TURN and STUN Server. Coturn before version 4.5.2 by default does not allow peers to connect and relay packets to loopback addresses in the range of `127.x.x.x`. However, it was observed that when sending a `CONNECT` request with the `XOR-PEER-ADDRESS` value of `0.0.0.0`, a successful response was received and subsequently, `CONNECTIONBIND` also received a successful response. Coturn then is able to relay packets to the loopback interface. Additionally, when coturn is listening on IPv6, which is default, the loopback interface can also be reached by making use of either `[::1]` or `[::]` as the peer address. By using the address `0.0.0.0` as the peer address, a malicious user will be able to relay packets to the loopback interface, unless `--denied-peer-ip=0.0.0.0` (or similar) has been specified. Since the default configuration implies that loopback peers are not allowed, coturn administrators may choose to not set the `denied-peer-ip` setting. The issue patched in version 4.5.2. As a workaround the addresses in the address block `0.0.0.0/8`, `[::1]` and `[::]` should be denied by default unless `--allow-loopback-peers` has been specified.
CVE-2020-2654	Vulnerability in the Java SE product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using

	Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2655	Vulnerability in the Java SE product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 11.0.5 and 13.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data as well as unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-2659	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u241 and 8u231; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-26950	In certain circumstances, the MCallGetProperty opcode can be emitted with unmet assumptions resulting in an exploitable use-after-free condition. This vulnerability affects Firefox < 82.0.3, Firefox ESR < 78.4.1, and Thunderbird < 78.4.2.
CVE-2020-26951	A parsing and event loading mismatch in Firefox's SVG code could have allowed load events to fire, even after sanitization. An attacker already capable of exploiting

	an XSS vulnerability in privileged internal pages could have used this attack to bypass our built-in sanitizer. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26952	Incorrect bookkeeping of functions inlined during JIT compilation could have led to memory corruption and a potentially exploitable crash when handling out-of-memory errors. This vulnerability affects Firefox < 83.
CVE-2020-26953	It was possible to cause the browser to enter fullscreen mode without displaying the security UI; thus making it possible to attempt a phishing attack or otherwise confuse the user. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26956	In some cases, removing HTML elements during sanitization would keep existing SVG event handlers and therefore lead to XSS. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26958	Firefox did not block execution of scripts with incorrect MIME types when the response was intercepted and cached through a ServiceWorker. This could lead to a cross-site script inclusion vulnerability, or a Content Security Policy bypass. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26959	During browser shutdown, reference decrementing could have occured on a previously freed object, resulting in a use-after-free, memory corruption, and a potentially exploitable crash. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26960	If the Compact() method was called on an nsTArray, the array could have been reallocated without updating other pointers, leading to a potential use-after-free and exploitable crash. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26961	When DNS over HTTPS is in use, it intentionally filters RFC1918 and related IP ranges from the responses as these do not make sense coming from a DoH resolver. However when an IPv4 address was mapped through IPv6, these addresses were erroneously let through, leading to a potential DNS Rebinding attack. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26962	Cross-origin iframes that contained a login form could have been recognized by the login autofill service, and populated. This could have been used in clickjacking attacks, as well as be read across partitions in dynamic first party isolation. This vulnerability affects Firefox < 83.

CVE-2020-26963	Repeated calls to the history and location interfaces could have been used to hang the browser. This was addressed by introducing rate-limiting to these API calls. This vulnerability affects Firefox < 83.
CVE-2020-26965	Some websites have a feature "Show Password" where clicking a button will change a password field into a textbook field, revealing the typed password. If, when using a software keyboard that remembers user input, a user typed their password and used that feature, the type of the password field was changed, resulting in a keyboard layout change and the possibility for the software keyboard to remember the typed password. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26967	When listening for page changes with a Mutation Observer, a malicious web page could confuse Firefox Screenshots into interacting with elements other than those that it injected into the page. This would lead to internal errors and unexpected behavior in the Screenshots code. This vulnerability affects Firefox < 83.
CVE-2020-26968	Mozilla developers reported memory safety bugs present in Firefox 82 and Firefox ESR 78.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26969	Mozilla developers reported memory safety bugs present in Firefox 82. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 83.
CVE-2020-26971	Certain blit values provided by the user were not properly constrained leading to a heap buffer overflow on some video drivers. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.
CVE-2020-26972	The lifecycle of IPC Actors allows managed actors to outlive their manager actors; and the former must ensure that they are not attempting to use a dead actor they have a reference to. Such a check was omitted in WebGL, resulting in a use-after-free and a potentially exploitable crash. This vulnerability affects Firefox < 84.
CVE-2020-26973	Certain input to the CSS Sanitizer confused it, resulting in incorrect components being removed. This could have been used as a sanitizer bypass. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.

CVE-2020-26974	When flex-basis was used on a table wrapper, a StyleGenericFlexBasis object could have been incorrectly cast to the wrong type. This resulted in a heap user-after-free, memory corruption, and a potentially exploitable crash. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.
CVE-2020-26976	When a HTTPS pages was embedded in a HTTP page, and there was a service worker registered for the former, the service worker could have intercepted the request for the secure page despite the iframe not being a secure context due to the (insecure) framing. This vulnerability affects Firefox < 84.
CVE-2020-26978	Using techniques that built on the slipstream research, a malicious webpage could have exposed both an internal network's hosts as well as services running on the user's local machine. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.
CVE-2020-26979	When a user typed a URL in the address bar or the search bar and quickly hit the enter key, a website could sometimes capture that event and then redirect the user before navigation occurred to the desired, entered address. To construct a convincing spoof the attacker would have had to guess what the user was typing, perhaps by suggesting it. This vulnerability affects Firefox < 84.
CVE-2020-27152	An issue was discovered in ioapic_lazy_update_eoi in arch/x86/kvm/ioapic.c in the Linux kernel before 5.9.2. It has an infinite loop related to improper interaction between a resampler and edge triggering, aka CID-77377064c3a9.
CVE-2020-2731	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Core RDBMS executes to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Core RDBMS accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Core RDBMS. CVSS 3.0 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L).
CVE-2020-2734	Vulnerability in the RDBMS/Optimizer component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged

	attacker having Execute on DBMS_SQLTUNE privilege with network access via Oracle Net to compromise RDBMS/Optimizer. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of RDBMS/ Optimizer accessible data. CVSS 3.0 Base Score 2.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/ AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N).
CVE-2020-27347	In tmux before version 3.1c the function input_csi_dispatch_sgr_colon() in file input.c contained a stack-based buffer-overflow that can be exploited by terminal output.
CVE-2020-27349	Aptdaemon performed policykit checks after interacting with potentially untrusted files with elevated privileges. This affected versions prior to 1.1.1+bzr982-0ubuntu34.1, 1.1.1+bzr982-0ubuntu32.3, 1.1.1+bzr982-0ubuntu19.5, 1.1.1+bzr982-0ubuntu14.5.
CVE-2020-2735	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Java VM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java VM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.0 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/ C:H/I:H/A:H).
CVE-2020-27350	APT had several integer overflows and underflows while parsing .deb packages, aka GHSL-2020-168 GHSL-2020-169, in files apt-pkg/contrib/extracttar.cc, apt-pkg/deb/debfile.cc, and apt-pkg/contrib/arfile.cc. This issue affects: apt 1.2.32ubuntu0 versions prior to 1.2.32ubuntu0.2; 1.6.12ubuntu0 versions prior to 1.6.12ubuntu0.2; 2.0.2ubuntu0 versions prior to 2.0.2ubuntu0.2; 2.1.10ubuntu0 versions prior to 2.1.10ubuntu0.1;
CVE-2020-27351	Various memory and file descriptor leaks were found in apt-python files python/arfile.cc, python/tag.cc, python/tarfile.cc, aka GHSL-2020-170. This issue affects: python-apt 1.1.0~beta1 versions prior to 1.1.0~beta1ubuntu0.16.04.10; 1.6.5ubuntu0 versions prior to 1.6.5ubuntu0.4; 2.0.0ubuntu0 versions prior to 2.0.0ubuntu0.20.04.2; 2.1.3ubuntu1 versions prior to 2.1.3ubuntu1.1;
CVE-2020-2737	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected

	are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows high privileged attacker having Create Session, Execute Catalog Role privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Core RDBMS. CVSS 3.0 Base Score 6.4 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).
CVE-2020-2752	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.47 and prior, 5.7.27 and prior and 8.0.17 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2754	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions that are affected are Java SE: 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2755	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions that are affected are Java SE: 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to

	client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2756	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-27560	ImageMagick 7.0.10-34 allows Division by Zero in OptimizeLayerFrames in MagickCore/layer.c, which may cause a denial of service.
CVE-2020-2757	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2759	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported

	versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2760	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2020-27616	ati_2d_blt in hw/display/ati_2d.c in QEMU 4.2.1 can encounter an outside-limits situation in a calculation. A guest can crash the QEMU process.
CVE-2020-27617	eth_get_gso_type in net/eth.c in QEMU 4.2.1 allows guest OS users to trigger an assertion failure. A guest can crash the QEMU process via packet data that lacks a valid Layer 3 protocol.
CVE-2020-27619	In Python 3 through 3.9.0, the Lib/test/multibytecodec_support.py CJK codec tests call eval() on content retrieved via HTTP.
CVE-2020-2762	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2763	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or

	frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-27638	receive.c in fastd before v21 allows denial of service (assertion failure) when receiving packets with an invalid type code.
CVE-2020-2765	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2766	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-2767	Vulnerability in the Java SE product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 11.0.6 and 14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data as well as unauthorized read access to a subset of Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-27673	An issue was discovered in the Linux kernel through 5.9.1, as used with Xen through 4.14.x. Guest OS users

	can cause a denial of service (host OS hang) via a high rate of events to dom0, aka CID-e99502f76271.
CVE-2020-27675	An issue was discovered in the Linux kernel through 5.9.1, as used with Xen through 4.14.x. drivers/xen/events/events_base.c allows event-channel removal during the event-handling loop (a race condition). This can cause a use-after-free or NULL pointer dereference, as demonstrated by a dom0 crash via events for an in-reconfiguration paravirtualized device, aka CID-073d0552ead5.
CVE-2020-2773	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-27777	A flaw was found in the way RTAS handled memory accesses in userspace to kernel communication. On a locked down (usually due to Secure Boot) guest system running on top of PowerVM or KVM hypervisors (pseries platform) a root like local user could use this flaw to further increase their privileges to that of a running kernel.
CVE-2020-2778	Vulnerability in the Java SE product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 11.0.6 and 14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Confidentiality

	impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-27783	A XSS vulnerability was discovered in python-lxml's clean module. The module's parser didn't properly imitate browsers, which caused different behaviors between the sanitizer and the user's page. A remote attacker could exploit this flaw to run arbitrary HTML/JS code.
CVE-2020-2780	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2781	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-27814	A heap-buffer overflow was found in the way openjpeg2 handled certain PNG format files. An attacker could use this flaw to cause an application crash or in some cases execute arbitrary code with the permission of the user running such an application.
CVE-2020-27815	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-27821	A flaw was found in the memory management API of QEMU during the initialization of a memory region

	cache. This issue could lead to an out-of-bounds write access to the MSI-X table while performing MMIO operations. A guest user may abuse this flaw to crash the QEMU process on the host, resulting in a denial of service. This flaw affects QEMU versions prior to 5.2.0.
CVE-2020-27823	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-27824	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-27827	A flaw was found in multiple versions of OpenvSwitch. Specially crafted LLDP packets can cause memory to be lost when allocating data to handle specific optional TLVs, potentially causing a denial of service. The highest threat from this vulnerability is to system availability.
CVE-2020-27830	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-27835	A use after free in the Linux kernel infiniband hfi1 driver in versions prior to 5.10-rc6 was found in the way user calls Ioctl after open dev file and fork. A local user could use this flaw to crash the system.
CVE-2020-27841	There's a flaw in openjpeg in versions prior to 2.4.0 in src/lib/openjp2/pi.c. When an attacker is able to provide crafted input to be processed by the openjpeg encoder, this could cause an out-of-bounds read. The greatest impact from this flaw is to application availability.
CVE-2020-27842	There's a flaw in openjpeg's t2 encoder in versions prior to 2.4.0. An attacker who is able to provide crafted input to be processed by openjpeg could cause a null pointer dereference. The highest impact of this flaw is to application availability.
CVE-2020-27843	A flaw was found in OpenJPEG in versions prior to 2.4.0. This flaw allows an attacker to provide specially crafted input to the conversion or encoding functionality, causing an out-of-bounds read. The highest threat from this vulnerability is system availability.
CVE-2020-27844	A flaw was found in openjpeg's src/lib/openjp2/t2.c in versions prior to 2.4.0. This flaw allows an attacker to provide crafted input to openjpeg during conversion and encoding, causing an out-of-bounds write. The

	highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2020-27845	There's a flaw in src/lib/openjp2/pi.c of openjpeg in versions prior to 2.4.0. If an attacker is able to provide untrusted input to openjpeg's conversion/encoding functionality, they could cause an out-of-bounds read. The highest impact of this flaw is to application availability.
CVE-2020-2798	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: WLS Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-2800	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-2801	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. Note: The patch for this issue will address the vulnerability only if the WLS instance is using JDK 1.7.0_191 or later, or JDK 1.8.0_181 or later. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability

	impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-2803	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2020-2804	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Memcached). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2805	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments,

	typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2020-2811	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Oracle WebLogic Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 6.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N).
CVE-2020-2812	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2814	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.6.47 and prior, 5.7.28 and prior and 8.0.18 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVE-2020-2816	Vulnerability in the Java SE product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 11.0.6 and 14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).
CVE-2020-28196	MIT Kerberos 5 (aka krb5) before 1.17.2 and 1.18.x before 1.18.3 allows unbounded recursion via an ASN.1-encoded Kerberos message because the lib/krb5/asn.1/asn1_encode.c support for BER indefinite lengths lacks a recursion limit.
CVE-2020-28241	libmaxminddb before 1.4.3 has a heap-based buffer over-read in dump_entry_data_list in maxminddb.c.
CVE-2020-2828	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: WLS Web Services). The supported version that is affected is 10.3.6.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2020-2829	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Management Services). The supported version that is affected is 10.3.6.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).
CVE-2020-2830	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Concurrency). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can

	result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-28374	In drivers/target/target_core_xcopy.c in the Linux kernel before 5.10.7, insufficient identifier checking in the LIO SCSI target code can be used by remote attackers to read or write files via directory traversal in an XCOPY request, aka CID-2896c93811e3. For example, an attack can occur over a network if the attacker has access to one iSCSI LUN. The attacker gains control over file access because I/O operations are proxied via an attacker-selected backstore.
CVE-2020-28588	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-2867	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Container). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.0 Base Score 8.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N).
CVE-2020-2869	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data. CVSS

	3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2020-2883	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-2884	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-28896	Mutt before 2.0.2 and NeoMutt before 2020-11-20 did not ensure that $ssl_force_tls was processed if an IMAP server's initial server response was invalid. The connection was not properly closed, and the code could continue attempting to authenticate. This could result in authentication credentials being exposed on an unencrypted connection, or to a machine-in-the-middle.
CVE-2020-28915	A buffer over-read (at the framebuffer layer) in the fbcon code in the Linux kernel before 5.8.15 could be used by local attackers to read kernel memory, aka CID-6735b4632def.
CVE-2020-28916	hw/net/e1000e_core.c in QEMU 5.0.0 has an infinite loop via an RX descriptor with a NULL buffer address.
CVE-2020-2892	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-28926	ReadyMedia (aka MiniDLNA) before versions 1.3.0 allows remote code execution. Sending a malicious UPnP HTTP request to the miniDLNA service using

	HTTP chunked encoding can lead to a signedness bug resulting in a buffer overflow in calls to memcpy/memmove.
CVE-2020-2893	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-28941	An issue was discovered in drivers/accessibility/speakup/spk_ttyio.c in the Linux kernel through 5.9.9. Local attackers on systems with the speakup driver could cause a local denial of service attack, aka CID-d41227544427. This occurs because of an invalid free when the line discipline is used more than once.
CVE-2020-28948	Archive_Tar through 1.4.10 allows an unserialization attack because phar: is blocked but PHAR: is not blocked.
CVE-2020-28949	Archive_Tar through 1.4.10 has :// filename sanitization only to address phar attacks, and thus any other stream-wrapper attack (such as file:// to overwrite files) can still succeed.
CVE-2020-2895	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2896	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Information Schema). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2897	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported

	versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-28974	A slab-out-of-bounds read in fbcon in the Linux kernel before 5.9.7 could be used by local attackers to read privileged information or potentially crash the kernel, aka CID-3c4e0dff2095. This occurs because KD_FONT_OP_COPY in drivers/tty/vt/vt.c can be used for manipulations such as font height.
CVE-2020-2898	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Charsets). The supported version that is affected is 8.0.19. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2901	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2903	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Connection Handling). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2904	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior.

	Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2921	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication Plugin). Supported versions that are affected are 8.0.19 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2922	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.18 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Client accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-2923	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2924	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability

	impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2925	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PS). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2926	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Group Replication GCS). Supported versions that are affected are 8.0.19 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2928	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2930	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 8.0.19 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-29361	An issue was discovered in p11-kit 0.21.1 through 0.23.21. Multiple integer overflows have been discovered in the array allocations in the p11-kit library and the p11-kit list command, where overflow checks are missing before calling realloc or calloc.

CVE-2020-29362	An issue was discovered in p11-kit 0.21.1 through 0.23.21. A heap-based buffer over-read has been discovered in the RPC protocol used by thep11-kit server/remote commands and the client library. When the remote entity supplies a byte array through a serialized PKCS#11 function call, the receiving entity may allow the reading of up to 4 bytes of memory past the heap allocation.
CVE-2020-29363	An issue was discovered in p11-kit 0.23.6 through 0.23.21. A heap-based buffer overflow has been discovered in the RPC protocol used by p11-kit server/remote commands and the client library. When the remote entity supplies a serialized byte array in a CK_ATTRIBUTE, the receiving entity may not allocate sufficient length for the buffer to store the deserialized value.
CVE-2020-29368	An issue was discovered in __split_huge_pmd in mm/huge_memory.c in the Linux kernel before 5.7.5. The copy-on-write implementation can grant unintended write access because of a race condition in a THP mapcount check, aka CID-c444eb564fb1.
CVE-2020-29369	An issue was discovered in mm/mmap.c in the Linux kernel before 5.7.11. There is a race condition between certain expand functions (expand_downwards and expand_upwards) and page-table free operations from an munmap call, aka CID-246c320a8cfe.
CVE-2020-29371	An issue was discovered in romfs_dev_read in fs/romfs/storage.c in the Linux kernel before 5.8.4. Uninitialized memory leaks to userspace, aka CID-bcf85fcedfdd.
CVE-2020-29385	GNOME gdk-pixbuf (aka GdkPixbuf) before 2.42.2 allows a denial of service (infinite loop) in lzw.c in the function write_indexes. if c->self_code equals 10, self->code_table[10].extends will assign the value 11 to c. The next execution in the loop will assign self->code_table[11].extends to c, which will give the value of 10. This will make the loop run infinitely. This bug can, for example, be triggered by calling this function with a GIF image with LZW compression that is crafted in a special way.
CVE-2020-29443	ide_atapi_cmd_reply_end in hw/ide/atapi.c in QEMU 5.1.0 allows out-of-bounds read access because a buffer index is not validated.
CVE-2020-29565	An issue was discovered in OpenStack Horizon before 15.3.2, 16.x before 16.2.1, 17.x and 18.x before 18.3.3, 18.4.x, and 18.5.x. There is a lack of validation of the "next" parameter, which would allow someone to supply a malicious URL in Horizon that can cause an automatic redirect to the provided malicious URL.
CVE-2020-29568	An issue was discovered in Xen through 4.14.x. Some OSes (such as Linux, FreeBSD, and NetBSD)

	are processing watch events using a single thread. If the events are received faster than the thread is able to handle, they will get queued. As the queue is unbounded, a guest may be able to trigger an OOM in the backend. All systems with a FreeBSD, Linux, or NetBSD (any version) dom0 are vulnerable.
CVE-2020-29569	An issue was discovered in the Linux kernel through 5.10.1, as used with Xen through 4.14.x. The Linux kernel PV block backend expects the kernel thread handler to reset ring->xenblkd to NULL when stopped. However, the handler may not have time to run if the frontend quickly toggles between the states connect and disconnect. As a consequence, the block backend may re-use a pointer after it was freed. A misbehaving guest can trigger a dom0 crash by continuously connecting / disconnecting a block frontend. Privilege escalation and information leaks cannot be ruled out. This only affects systems with a Linux blkback.
CVE-2020-2963	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows high privileged attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.0 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-2966	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0 and 12.2.1.4.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle WebLogic Server accessible data as well as unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N).
CVE-2020-29660	A locking inconsistency issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_io.c and drivers/tty/tty_jobctrl.c may allow a read-after-free attack against TIOCGSID, aka CID-c8bcd9c5be24.

CVE-2020-29661	A locking issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_jobctrl.c allows a use-after-free attack against TIOCSPGRP, aka CID-54ffccbf053b.
CVE-2020-2967	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2020-2968	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java VM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H).
CVE-2020-2969	Vulnerability in the Data Pump component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows high privileged attacker having DBA role account privilege with network access via Oracle Net to compromise Data Pump. Successful attacks of this vulnerability can result in takeover of Data Pump. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-2978	Vulnerability in the Oracle Database - Enterprise Edition component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having DBA role account privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition. While the vulnerability is in Oracle Database - Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of

	Oracle Database - Enterprise Edition accessible data. CVSS 3.1 Base Score 4.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:L/A:N).
CVE-2020-3327	A vulnerability in the ARJ archive parsing module in Clam AntiVirus (ClamAV) Software versions 0.102.2 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to a heap buffer overflow read. An attacker could exploit this vulnerability by sending a crafted ARJ file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition.
CVE-2020-3341	A vulnerability in the PDF archive parsing module in Clam AntiVirus (ClamAV) Software versions 0.101 - 0.102.2 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to a stack buffer overflow read. An attacker could exploit this vulnerability by sending a crafted PDF file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition.
CVE-2020-3350	A vulnerability in the endpoint software of Cisco AMP for Endpoints and Clam AntiVirus could allow an authenticated, local attacker to cause the running software to delete arbitrary files on the system. The vulnerability is due to a race condition that could occur when scanning malicious files. An attacker with local shell access could exploit this vulnerability by executing a script that could trigger the race condition. A successful exploit could allow the attacker to delete arbitrary files on the system that the attacker would not normally have privileges to delete, producing system instability or causing the endpoint software to stop working.
CVE-2020-3481	A vulnerability in the EGG archive parsing module in Clam AntiVirus (ClamAV) Software versions 0.102.0 - 0.102.3 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to a null pointer dereference. An attacker could exploit this vulnerability by sending a crafted EGG file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial of service condition.
CVE-2020-35111	When an extension with the proxy permission registered to receive <all_urls>, the proxy.onRequest callback was not triggered for view-source URLs. While web content cannot navigate to such URLs, a user

	opening View Source could have inadvertently leaked their IP address. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.
CVE-2020-35113	Mozilla developers reported memory safety bugs present in Firefox 83 and Firefox ESR 78.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.
CVE-2020-35114	Mozilla developers reported memory safety bugs present in Firefox 83. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 84.
CVE-2020-35498	A vulnerability was found in openvswitch. A limitation in the implementation of userspace packet parsing can allow a malicious user to send a specially crafted packet causing the resulting megaflow in the kernel to be too wide, potentially causing a denial of service. The highest threat from this vulnerability is to system availability.
CVE-2020-35508	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2020-35523	An integer overflow flaw was found in libtiff that exists in the tif_getimage.c file. This flaw allows an attacker to inject and execute arbitrary code when a user opens a crafted TIFF file. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2020-35524	A heap-based buffer overflow flaw was found in libtiff in the handling of TIFF images in libtiff's TIFF2PDF tool. A specially crafted TIFF file can lead to arbitrary code execution. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2020-35653	In Pillow before 8.1.0, PcxDecode has a buffer over-read when decoding a crafted PCX file because the user-supplied stride value is trusted for buffer calculations.
CVE-2020-35654	In Pillow before 8.1.0, TiffDecode has a heap-based buffer overflow when decoding crafted YCbCr files because of certain interpretation conflicts with LibTIFF in RGBA mode.
CVE-2020-35655	In Pillow before 8.1.0, SGIRleDecode has a 4-byte buffer over-read when decoding crafted SGI RLE image files because offsets and length tables are mishandled.

CVE-2020-35738	WavPack 5.3.0 has an out-of-bounds write in WavpackPackSamples in pack_utils.c because of an integer overflow in a malloc argument. NOTE: some third-parties claim that there are later "unofficial" releases through 5.3.2, which are also affected.
CVE-2020-36158	mwifiex_cmd_802_11_ad_hoc_start in drivers/net/wireless/marvell/mwifiex/join.c in the Linux kernel through 5.10.4 might allow remote attackers to execute arbitrary code via a long SSID value, aka CID-5c455c5ab332.
CVE-2020-36193	Tar.php in Archive_Tar through 1.4.11 allows write operations with Directory Traversal due to inadequate checking of symbolic links, a related issue to CVE-2020-28948.
CVE-2020-36221	An integer underflow was discovered in OpenLDAP before 2.4.57 leading to slapd crashes in the Certificate Exact Assertion processing, resulting in denial of service (schema_init.c serialNumberAndIssuerCheck).
CVE-2020-36222	A flaw was discovered in OpenLDAP before 2.4.57 leading to an assertion failure in slapd in the saslAuthzTo validation, resulting in denial of service.
CVE-2020-36223	A flaw was discovered in OpenLDAP before 2.4.57 leading to a slapd crash in the Values Return Filter control handling, resulting in denial of service (double free and out-of-bounds read).
CVE-2020-36224	A flaw was discovered in OpenLDAP before 2.4.57 leading to an invalid pointer free and slapd crash in the saslAuthzTo processing, resulting in denial of service.
CVE-2020-36225	A flaw was discovered in OpenLDAP before 2.4.57 leading to a double free and slapd crash in the saslAuthzTo processing, resulting in denial of service.
CVE-2020-36226	A flaw was discovered in OpenLDAP before 2.4.57 leading to a memch->bv_len miscalculation and slapd crash in the saslAuthzTo processing, resulting in denial of service.
CVE-2020-36227	A flaw was discovered in OpenLDAP before 2.4.57 leading to an infinite loop in slapd with the cancel_extop Cancel operation, resulting in denial of service.
CVE-2020-36228	An integer underflow was discovered in OpenLDAP before 2.4.57 leading to a slapd crash in the Certificate List Exact Assertion processing, resulting in denial of service.
CVE-2020-36229	A flaw was discovered in ldap_X509dn2bv in OpenLDAP before 2.4.57 leading to a slapd crash in the X.509 DN parsing in ad_keystring, resulting in denial of service.
CVE-2020-36230	A flaw was discovered in OpenLDAP before 2.4.57 leading in an assertion failure in slapd in the X.509

	DN parsing in decode.c ber_next_element, resulting in denial of service.
CVE-2020-36241	autoar-extractor.c in GNOME gnome-autoar through 0.2.4, as used by GNOME Shell, Nautilus, and other software, allows Directory Traversal during extraction because it lacks a check of whether a file's parent is a symlink to a directory outside of the intended extraction location.
CVE-2020-3757	Adobe Flash Player versions 32.0.0.321 and earlier, 32.0.0.314 and earlier, 32.0.0.321 and earlier, and 32.0.0.255 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2020-3810	Missing input validation in the ar/tar implementations of APT before version 2.1.2 could result in denial of service when processing specially crafted deb files.
CVE-2020-3811	qmail-verify as used in netqmail 1.06 is prone to a mail-address verification bypass vulnerability.
CVE-2020-3812	qmail-verify as used in netqmail 1.06 is prone to an information disclosure vulnerability. A local attacker can test for the existence of files and directories anywhere in the filesystem because qmail-verify runs as root and tests for the existence of files in the attacker's home directory, without dropping its privileges first.
CVE-2020-3898	A memory corruption issue was addressed with improved validation. This issue is fixed in macOS Catalina 10.15.4. An application may be able to gain elevated privileges.
CVE-2020-3899	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution.
CVE-2020-4006	VMware Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector address have a command injection vulnerability.
CVE-2020-4030	In FreeRDP before version 2.1.2, there is an out of bounds read in TrioParse. Logging might bypass string length checks due to an integer overflow. This is fixed in version 2.1.2.
CVE-2020-4031	In FreeRDP before version 2.1.2, there is a use-after-free in gdi_SelectObject. All FreeRDP clients using compatibility mode with /relax-order-checks are affected. This is fixed in version 2.1.2.
CVE-2020-4032	In FreeRDP before version 2.1.2, there is an integer casting vulnerability in update_recv_secondary_order. All clients with +glyph-cache /relax-order-checks are affected. This is fixed in version 2.1.2.

CVE-2020-4033	In FreeRDP before version 2.1.2, there is an out of bounds read in RLEDECOMPRESS. All FreeRDP based clients with sessions with color depth < 32 are affected. This is fixed in version 2.1.2.
CVE-2020-4054	In Sanitize (RubyGem sanitize) greater than or equal to 3.0.0 and less than 5.2.1, there is a cross-site scripting vulnerability. When HTML is sanitized using Sanitize's "relaxed" config, or a custom config that allows certain elements, some content in a math or svg element may not be sanitized correctly even if math and svg are not in the allowlist. You are likely to be vulnerable to this issue if you use Sanitize's relaxed config or a custom config that allows one or more of the following HTML elements: iframe, math, noembed, noframes, noscript, plaintext, script, style, svg, xmp. Using carefully crafted input, an attacker may be able to sneak arbitrary HTML through Sanitize, potentially resulting in XSS (cross-site scripting) or other undesired behavior when that HTML is rendered in a browser. This has been fixed in 5.2.1.
CVE-2020-4067	In coturn before version 4.5.1.3, there is an issue whereby STUN/TURN response buffer is not initialized properly. There is a leak of information between different client connections. One client (an attacker) could use their connection to intelligently query coturn to get interesting bytes in the padding bytes from the connection of another client. This has been fixed in 4.5.1.3.
CVE-2020-4163	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0, under specialized conditions, could allow an authenticated user to create a maliciously crafted file name which would be misinterpreted as jsp content and executed. IBM X-Force ID: 174397.
CVE-2020-4276	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional is vulnerable to a privilege escalation vulnerability when using token-based authentication in an admin request over the SOAP connector. X-Force ID: 175984.
CVE-2020-4329	IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0 and Liberty 17.0.0.3 through 20.0.0.4 could allow a remote, authenticated attacker to obtain sensitive information, caused by improper parameter checking. This could be exploited to conduct spoofing attacks. IBM X-Force ID: 177841.
CVE-2020-4362	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional is vulnerable to a privilege escalation vulnerability when using token-based authentication in an admin request over the SOAP connector. IBM X-Force ID: 178929.
CVE-2020-4365	IBM WebSphere Application Server 8.5 is vulnerable to server-side request forgery. By sending a specially

	crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 178964.
CVE-2020-4448	IBM WebSphere Application Server Network Deployment 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects from untrusted sources. IBM X-Force ID: 181228.
CVE-2020-4449	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional could allow a remote attacker to obtain sensitive information with a specially-crafted sequence of serialized objects. IBM X-Force ID: 181230.
CVE-2020-4450	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects. IBM X-Force ID: 181231.
CVE-2020-4464	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional could allow a remote attacker to execute arbitrary code on a system with a specially-crafted sequence of serialized objects over the SOAP connector. IBM X-Force ID: 181489.
CVE-2020-4534	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a local authenticated attacker to gain elevated privileges on the system, caused by improper handling of UNC paths. By scheduling a task with a specially-crafted UNC path, an attacker could exploit this vulnerability to execute arbitrary code with higher privileges. IBM X-Force ID: 182808.
CVE-2020-4575	IBM WebSphere Application Server ND 8.5 and 9.0, and IBM WebSphere Virtual Enterprise 7.0 and 8.0 are vulnerable to cross-site scripting when High Availability Deployment Manager is configured.
CVE-2020-4578	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 184433.
CVE-2020-4589	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects from untrusted sources. IBM X-Force ID: 184585.
CVE-2020-4643	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information. IBM X-Force ID: 185590.

CVE-2020-4788	IBM Power9 (AIX 7.1, 7.2, and VIOS 3.1) processors could allow a local user to obtain sensitive information from the data in the L1 cache under extenuating circumstances. IBM X-Force ID: 189296.
CVE-2020-4949	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 192025.
CVE-2020-5421	In Spring Framework versions 5.2.0 - 5.2.8, 5.1.0 - 5.1.17, 5.0.0 - 5.0.18, 4.3.0 - 4.3.28, and older unsupported versions, the protections against RFD attacks from CVE-2015-5211 may be bypassed depending on the browser used through the use of a jsessionid path parameter.
CVE-2020-5963	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the Inter Process Communication APIs, in which improper access control may lead to code execution, denial of service, or information disclosure.
CVE-2020-5967	NVIDIA Linux GPU Display Driver, all versions, contains a vulnerability in the UVM driver, in which a race condition may lead to a denial of service.
CVE-2020-5973	NVIDIA Virtual GPU Manager and the guest drivers contain a vulnerability in vGPU plugin, in which there is the potential to execute privileged operations, which may lead to denial of service. This affects vGPU version 8.x (prior to 8.4), version 9.x (prior to 9.4) and version 10.x (prior to 10.3).
CVE-2020-6061	An exploitable heap overflow vulnerability exists in the way CoTURN 4.5.1.1 web server parses POST requests. A specially crafted HTTP POST request can lead to information leaks and other misbehavior. An attacker needs to send an HTTPS request to trigger this vulnerability.
CVE-2020-6062	An exploitable denial-of-service vulnerability exists in the way CoTURN 4.5.1.1 web server parses POST requests. A specially crafted HTTP POST request can lead to server crash and denial of service. An attacker needs to send an HTTP request to trigger this vulnerability.
CVE-2020-6377	Use after free in audio in Google Chrome prior to 79.0.3945.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6378	Use after free in speech in Google Chrome prior to 79.0.3945.130 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2020-6379	Use after free in V8 in Google Chrome prior to 79.0.3945.130 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6380	Insufficient policy enforcement in extensions in Google Chrome prior to 79.0.3945.130 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted Chrome Extension.
CVE-2020-6381	Integer overflow in JavaScript in Google Chrome on ChromeOS and Android prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6382	Type confusion in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6383	Type confusion in V8 in Google Chrome prior to 80.0.3987.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6384	Use after free in WebAudio in Google Chrome prior to 80.0.3987.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6385	Insufficient policy enforcement in storage in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2020-6386	Use after free in speech in Google Chrome prior to 80.0.3987.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6387	Out of bounds write in WebRTC in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted video stream.
CVE-2020-6388	Out of bounds access in WebAudio in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6389	Out of bounds write in WebRTC in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted video stream.
CVE-2020-6390	Out of bounds memory access in streams in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6391	Insufficient validation of untrusted input in Blink in Google Chrome prior to 80.0.3987.87 allowed a local attacker to bypass content security policy via a crafted HTML page.
CVE-2020-6392	Insufficient policy enforcement in extensions in Google Chrome prior to 80.0.3987.87 allowed an attacker who convinced a user to install a malicious extension to

	bypass navigation restrictions via a crafted Chrome Extension.
CVE-2020-6393	Insufficient policy enforcement in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6394	Insufficient policy enforcement in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2020-6395	Out of bounds read in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-6396	Inappropriate implementation in Skia in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-6397	Inappropriate implementation in sharing in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-6398	Use of uninitialized data in PDFium in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2020-6399	Insufficient policy enforcement in AppCache in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6400	Inappropriate implementation in CORS in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6401	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2020-6402	Insufficient policy enforcement in downloads in Google Chrome on OS X prior to 80.0.3987.87 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.
CVE-2020-6403	Incorrect implementation in Omnibox in Google Chrome on iOS prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-6404	Inappropriate implementation in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6405	Out of bounds read in SQLite in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to obtain

	potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-6406	Use after free in audio in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6407	Out of bounds memory access in streams in Google Chrome prior to 80.0.3987.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6408	Insufficient policy enforcement in CORS in Google Chrome prior to 80.0.3987.87 allowed a local attacker to obtain potentially sensitive information via a crafted HTML page.
CVE-2020-6409	Inappropriate implementation in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker who convinced the user to enter a URI to bypass navigation restrictions via a crafted domain name.
CVE-2020-6410	Insufficient policy enforcement in navigation in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to confuse the user via a crafted domain name.
CVE-2020-6411	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2020-6412	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2020-6413	Inappropriate implementation in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass HTML validators via a crafted HTML page.
CVE-2020-6414	Insufficient policy enforcement in Safe Browsing in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6415	Inappropriate implementation in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6416	Insufficient data validation in streams in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6417	Inappropriate implementation in installer in Google Chrome prior to 80.0.3987.87 allowed a local attacker to execute arbitrary code via a crafted registry entry.

CVE-2020-6418	Type confusion in V8 in Google Chrome prior to 80.0.3987.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6419	Out of bounds write in V8 in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6420	Insufficient policy enforcement in media in Google Chrome prior to 80.0.3987.132 allowed a remote attacker to bypass same origin policy via a crafted HTML page.
CVE-2020-6422	Use after free in WebGL in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6423	Use after free in audio in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6424	Use after free in media in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6425	Insufficient policy enforcement in extensions in Google Chrome prior to 80.0.3987.149 allowed an attacker who convinced a user to install a malicious extension to bypass site isolation via a crafted Chrome Extension.
CVE-2020-6426	Inappropriate implementation in V8 in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6427	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6428	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6429	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6430	Type Confusion in V8 in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6431	Insufficient policy enforcement in full screen in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-6432	Insufficient policy enforcement in navigations in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6433	Insufficient policy enforcement in extensions in Google Chrome prior to 81.0.4044.92 allowed a remote attacker

	to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6434	Use after free in devtools in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6435	Insufficient policy enforcement in extensions in Google Chrome prior to 81.0.4044.92 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6436	Use after free in window management in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6437	Inappropriate implementation in WebView in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to spoof security UI via a crafted application.
CVE-2020-6438	Insufficient policy enforcement in extensions in Google Chrome prior to 81.0.4044.92 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory via a crafted Chrome Extension.
CVE-2020-6439	Insufficient policy enforcement in navigations in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass security UI via a crafted HTML page.
CVE-2020-6440	Inappropriate implementation in extensions in Google Chrome prior to 81.0.4044.92 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information via a crafted Chrome Extension.
CVE-2020-6441	Insufficient policy enforcement in omnibox in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass security UI via a crafted HTML page.
CVE-2020-6442	Inappropriate implementation in cache in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6443	Insufficient data validation in developer tools in Google Chrome prior to 81.0.4044.92 allowed a remote attacker who had convinced the user to use devtools to execute arbitrary code via a crafted HTML page.
CVE-2020-6444	Uninitialized use in WebRTC in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6445	Insufficient policy enforcement in trusted types in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2020-6446	Insufficient policy enforcement in trusted types in Google Chrome prior to 81.0.4044.92 allowed a remote

	attacker to bypass content security policy via a crafted HTML page.
CVE-2020-6447	Inappropriate implementation in developer tools in Google Chrome prior to 81.0.4044.92 allowed a remote attacker who had convinced the user to use devtools to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6448	Use after free in V8 in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6449	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6450	Use after free in WebAudio in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6451	Use after free in WebAudio in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6452	Heap buffer overflow in media in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6453	Inappropriate implementation in V8 in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6454	Use after free in extensions in Google Chrome prior to 81.0.4044.92 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2020-6455	Out of bounds read in WebSQL in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6456	Insufficient validation of untrusted input in clipboard in Google Chrome prior to 81.0.4044.92 allowed a local attacker to bypass site isolation via crafted clipboard contents.
CVE-2020-6457	Use after free in speech recognizer in Google Chrome prior to 81.0.4044.113 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6458	Out of bounds read and write in PDFium in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.

CVE-2020-6459	Use after free in payments in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6460	Insufficient data validation in URL formatting in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to perform domain spoofing via a crafted domain name.
CVE-2020-6461	Use after free in storage in Google Chrome prior to 81.0.4044.129 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6462	Use after free in task scheduling in Google Chrome prior to 81.0.4044.129 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6463	Use after free in ANGLE in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6464	Type confusion in Blink in Google Chrome prior to 81.0.4044.138 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6465	Use after free in reader mode in Google Chrome on Android prior to 83.0.4103.61 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6466	Use after free in media in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6467	Use after free in WebRTC in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6468	Type confusion in V8 in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6469	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2020-6470	Insufficient validation of untrusted input in clipboard in Google Chrome prior to 83.0.4103.61 allowed a local attacker to inject arbitrary scripts or HTML (UXSS) via crafted clipboard contents.
CVE-2020-6471	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious

	extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2020-6472	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory or disk via a crafted Chrome Extension.
CVE-2020-6473	Insufficient policy enforcement in Blink in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-6474	Use after free in Blink in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6475	Incorrect implementation in full screen in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-6476	Insufficient policy enforcement in tab strip in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.
CVE-2020-6477	Inappropriate implementation in installer in Google Chrome on OS X prior to 83.0.4103.61 allowed a local attacker to perform privilege escalation via a crafted file.
CVE-2020-6478	Inappropriate implementation in full screen in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-6479	Inappropriate implementation in sharing in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-6480	Insufficient policy enforcement in enterprise in Google Chrome prior to 83.0.4103.61 allowed a local attacker to bypass navigation restrictions via UI actions.
CVE-2020-6481	Insufficient policy enforcement in URL formatting in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to perform domain spoofing via a crafted domain name.
CVE-2020-6482	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.
CVE-2020-6483	Insufficient policy enforcement in payments in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.

CVE-2020-6484	Insufficient data validation in ChromeDriver in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted request.
CVE-2020-6485	Insufficient data validation in media router in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6486	Insufficient policy enforcement in navigations in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6487	Insufficient policy enforcement in downloads in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6488	Insufficient policy enforcement in downloads in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6489	Inappropriate implementation in developer tools in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had convinced the user to take certain actions in developer tools to obtain potentially sensitive information from disk via a crafted HTML page.
CVE-2020-6490	Insufficient data validation in loader in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had been able to write to disk to leak cross-origin data via a crafted HTML page.
CVE-2020-6491	Insufficient data validation in site information in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted domain name.
CVE-2020-6493	Use after free in WebAuthentication in Google Chrome prior to 83.0.4103.97 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6494	Incorrect security UI in payments in Google Chrome on Android prior to 83.0.4103.97 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-6495	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.97 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2020-6496	Use after free in payments in Google Chrome on MacOS prior to 83.0.4103.97 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.

CVE-2020-6499	Inappropriate implementation in AppCache in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass AppCache security restrictions via a crafted HTML page.
CVE-2020-6500	Inappropriate implementation in interstitials in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-6501	Insufficient policy enforcement in CSP in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2020-6502	Incorrect implementation in permissions in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-6503	Inappropriate implementation in accessibility in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-6504	Insufficient policy enforcement in notifications in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass notification restrictions via a crafted HTML page.
CVE-2020-6505	Use after free in speech in Google Chrome prior to 83.0.4103.106 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6506	Insufficient policy enforcement in WebView in Google Chrome on Android prior to 83.0.4103.106 allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2020-6507	Out of bounds write in V8 in Google Chrome prior to 83.0.4103.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6509	Use after free in extensions in Google Chrome prior to 83.0.4103.116 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2020-6510	Heap buffer overflow in background fetch in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6511	Information leak in content security policy in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6512	Type Confusion in V8 in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2020-6513	Heap buffer overflow in PDFium in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2020-6514	Inappropriate implementation in WebRTC in Google Chrome prior to 84.0.4147.89 allowed an attacker in a privileged network position to potentially exploit heap corruption via a crafted SCTP stream.
CVE-2020-6515	Use after free in tab strip in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6516	Policy bypass in CORS in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6517	Heap buffer overflow in history in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6518	Use after free in developer tools in Google Chrome prior to 84.0.4147.89 allowed a remote attacker who had convinced the user to use developer tools to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6519	Policy bypass in CSP in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2020-6520	Buffer overflow in Skia in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6521	Side-channel information leakage in autofill in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-6522	Inappropriate implementation in external protocol handlers in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6523	Out of bounds write in Skia in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6524	Heap buffer overflow in WebAudio in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6525	Heap buffer overflow in Skia in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6526	Inappropriate implementation in iframe sandbox in Google Chrome prior to 84.0.4147.89 allowed a remote

	attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6527	Insufficient policy enforcement in CSP in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2020-6528	Incorrect security UI in basic auth in Google Chrome on iOS prior to 84.0.4147.89 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-6529	Inappropriate implementation in WebRTC in Google Chrome prior to 84.0.4147.89 allowed an attacker in a privileged network position to leak cross-origin data via a crafted HTML page.
CVE-2020-6530	Out of bounds memory access in developer tools in Google Chrome prior to 84.0.4147.89 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2020-6531	Side-channel information leakage in scroll to text in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6532	Use after free in SCTP in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6533	Type Confusion in V8 in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6534	Heap buffer overflow in WebRTC in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6535	Insufficient data validation in WebUI in Google Chrome prior to 84.0.4147.89 allowed a remote attacker who had compromised the renderer process to inject scripts or HTML into a privileged page via a crafted HTML page.
CVE-2020-6536	Incorrect security UI in PWAs in Google Chrome prior to 84.0.4147.89 allowed a remote attacker who had persuaded the user to install a PWA to spoof the contents of the Omnibox (URL bar) via a crafted PWA.
CVE-2020-6537	Type confusion in V8 in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2020-6538	Inappropriate implementation in WebView in Google Chrome on Android prior to 84.0.4147.105 allowed a

	remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6539	Use after free in CSS in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6540	Buffer overflow in Skia in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6541	Use after free in WebUSB in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6542	Use after free in ANGLE in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6543	Use after free in task scheduling in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6544	Use after free in media in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6545	Use after free in audio in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6546	Inappropriate implementation in installer in Google Chrome prior to 84.0.4147.125 allowed a local attacker to potentially elevate privilege via a crafted filesystem.
CVE-2020-6547	Incorrect security UI in media in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially obtain sensitive information via a crafted HTML page.
CVE-2020-6548	Heap buffer overflow in Skia in Google Chrome prior to 84.0.4147.125 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6549	Use after free in media in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6550	Use after free in IndexedDB in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6551	Use after free in WebXR in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6552	Use after free in Blink in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6553	Use after free in offline mode in Google Chrome on iOS prior to 84.0.4147.125 allowed a remote attacker to

	potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6554	Use after free in extensions in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2020-6555	Out of bounds read in WebGL in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-6556	Heap buffer overflow in SwiftShader in Google Chrome prior to 84.0.4147.135 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6557	Inappropriate implementation in networking in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2020-6559	Use after free in presentation API in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6560	Insufficient policy enforcement in autofill in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6561	Inappropriate implementation in Content Security Policy in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6562	Insufficient policy enforcement in Blink in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6563	Insufficient policy enforcement in intent handling in Google Chrome on Android prior to 85.0.4183.83 allowed a remote attacker to obtain potentially sensitive information from disk via a crafted HTML page.
CVE-2020-6564	Inappropriate implementation in permissions in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to spoof the contents of a permission dialog via a crafted HTML page.
CVE-2020-6565	Inappropriate implementation in Omnibox in Google Chrome on iOS prior to 85.0.4183.83 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-6566	Insufficient policy enforcement in media in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6567	Insufficient validation of untrusted input in command line handling in Google Chrome on Windows prior to

	85.0.4183.83 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6568	Insufficient policy enforcement in intent handling in Google Chrome on Android prior to 85.0.4183.83 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6569	Integer overflow in WebUSB in Google Chrome prior to 85.0.4183.83 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6570	Information leakage in WebRTC in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to obtain potentially sensitive information via a crafted WebRTC interaction.
CVE-2020-6571	Insufficient data validation in Omnibox in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2020-6572	Use after free in Media in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2020-6573	Use after free in video in Google Chrome on Android prior to 85.0.4183.102 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6574	Insufficient policy enforcement in installer in Google Chrome on OS X prior to 85.0.4183.102 allowed a local attacker to potentially achieve privilege escalation via a crafted binary.
CVE-2020-6575	Race in Mojo in Google Chrome prior to 85.0.4183.102 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6576	Use after free in offscreen canvas in Google Chrome prior to 85.0.4183.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6829	When performing EC scalar point multiplication, the wNAF point multiplication algorithm was used; which leaked partial information about the nonce used during signature generation. Given an electro-magnetic trace of a few signature generations, the private key could have been computed. This vulnerability affects Firefox < 80 and Firefox for Android < 80.
CVE-2020-6831	A buffer overflow could occur when parsing and validating SCTP chunks in WebRTC. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0.

CVE-2020-7009	Elasticsearch versions from 6.7.0 before 6.8.8 and 7.0.0 before 7.6.2 contain a privilege escalation flaw if an attacker is able to create API keys. An attacker who is able to generate an API key can perform a series of steps that result in an API key being generated with elevated privileges.
CVE-2020-7012	Kibana versions 6.7.0 to 6.8.8 and 7.0.0 to 7.6.2 contain a prototype pollution flaw in the Upgrade Assistant. An authenticated attacker with privileges to write to the Kibana index could insert data that would cause Kibana to execute arbitrary code. This could possibly lead to an attacker executing code with the permissions of the Kibana process on the host system.
CVE-2020-7013	Kibana versions before 6.8.9 and 7.7.0 contain a prototype pollution flaw in TSVB. An authenticated attacker with privileges to create TSVB visualizations could insert data that would cause Kibana to execute arbitrary code. This could possibly lead to an attacker executing code with the permissions of the Kibana process on the host system.
CVE-2020-7014	The fix for CVE-2020-7009 was found to be incomplete. Elasticsearch versions from 6.7.0 to 6.8.7 and 7.0.0 to 7.6.1 contain a privilege escalation flaw if an attacker is able to create API keys and also authentication tokens. An attacker who is able to generate an API key and an authentication token can perform a series of steps that result in an authentication token being generated with elevated privileges.
CVE-2020-7015	Kibana versions before 6.8.9 and 7.7.0 contains a stored XSS flaw in the TSVB visualization. An attacker who is able to edit or create a TSVB visualization could allow the attacker to obtain sensitive information from, or perform destructive actions, on behalf of Kibana users who edit the TSVB visualization.
CVE-2020-7016	Kibana versions before 6.8.11 and 7.8.1 contain a denial of service (DoS) flaw in Timelion. An attacker can construct a URL that when viewed by a Kibana user can lead to the Kibana process consuming large amounts of CPU and becoming unresponsive.
CVE-2020-7017	In Kibana versions before 6.8.11 and 7.8.1 the region map visualization in contains a stored XSS flaw. An attacker who is able to edit or create a region map visualization could obtain sensitive information or perform destructive actions on behalf of Kibana users who view the region map visualization.
CVE-2020-7019	In Elasticsearch before 7.9.0 and 6.8.12 a field disclosure flaw was found when running a scrolling search with Field Level Security. If a user runs the same query another more privileged user recently ran, the scrolling search can leak fields that should

	be hidden. This could result in an attacker gaining additional permissions against a restricted index.
CVE-2020-7020	Elasticsearch versions before 6.8.13 and 7.9.2 contain a document disclosure flaw when Document or Field Level Security is used. Search queries do not properly preserve security permissions when executing certain complex queries. This could result in the search disclosing the existence of documents the attacker should not be able to view. This could result in an attacker gaining additional insight into potentially sensitive indices.
CVE-2020-7040	storeBackup.pl in storeBackup through 3.5 relies on the /tmp/storeBackup.lock pathname, which allows symlink attacks that possibly lead to privilege escalation. (Local users can also create a plain file named /tmp/storeBackup.lock to block use of storeBackup until an admin manually deletes that file.)
CVE-2020-7064	In PHP versions 7.2.x below 7.2.9, 7.3.x below 7.3.16 and 7.4.x below 7.4.4, while parsing EXIF data with exif_read_data() function, it is possible for malicious data to cause PHP to read one byte of uninitialized memory. This could potentially lead to information disclosure or crash.
CVE-2020-7065	In PHP versions 7.3.x below 7.3.16 and 7.4.x below 7.4.4, while using mb_strtolower() function with UTF-32LE encoding, certain invalid strings could cause PHP to overwrite stack-allocated buffer. This could lead to memory corruption, crashes and potentially code execution.
CVE-2020-7066	In PHP versions 7.2.x below 7.2.29, 7.3.x below 7.3.16 and 7.4.x below 7.4.4, while using get_headers() with user-supplied URL, if the URL contains zero (\0) character, the URL will be silently truncated at it. This may cause some software to make incorrect assumptions about the target of the get_headers() and possibly send some information to a wrong server.
CVE-2020-7069	In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when AES-CCM mode is used with openssl_encrypt() function with 12 bytes IV, only first 7 bytes of the IV is actually used. This can lead to both decreased security and incorrect encryption data.
CVE-2020-7070	In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when PHP is processing incoming HTTP cookie values, the cookie names are url-decoded. This may lead to cookies with prefixes like __Host confused with cookies that decode to such prefix, thus leading to an attacker being able to forge cookie which is supposed to be secure. See also CVE-2020-8184 for more information.

CVE-2020-7663	websocket-extensions ruby module prior to 0.1.5 allows Denial of Service (DoS) via Regex Backtracking. The extension parser may take quadratic time when parsing a header containing an unclosed string parameter value whose content is a repeating two-byte sequence of a backslash and some other character. This could be abused by an attacker to conduct Regex Denial Of Service (ReDoS) on a single-threaded server by providing a malicious payload with the Sec-WebSocket-Extensions header.
CVE-2020-8112	opj_t1_clbl_decode_processor in openjp2/t1.c in OpenJPEG 2.3.1 through 2020-01-28 has a heap-based buffer overflow in the qmfbid==1 case, a different issue than CVE-2020-6851.
CVE-2020-8169	curl 7.62.0 through 7.70.0 is vulnerable to an information disclosure vulnerability that can lead to a partial password being leaked over the network and to the DNS server(s).
CVE-2020-8177	curl 7.20.0 through 7.70.0 is vulnerable to improper restriction of names for files and other resources that can lead too overwriting a local file when the -J flag is used.
CVE-2020-8231	Due to use of a dangling pointer, libcurl 7.29.0 through 7.71.1 can use the wrong connection when sending data.
CVE-2020-8252	The implementation of realpath in libuv < 10.22.1, < 12.18.4, and < 14.9.0 used within Node.js incorrectly determined the buffer size which can result in a buffer overflow if the resolved path is longer than 256 bytes.
CVE-2020-8284	A malicious server can use the FTP PASV response to trick curl 7.73.0 and earlier into connecting back to a given IP address and port, and this way potentially make curl extract information about services that are otherwise private and not disclosed, for example doing port scanning and service banner extractions.
CVE-2020-8285	curl 7.21.0 to and including 7.73.0 is vulnerable to uncontrolled recursion due to a stack overflow issue in FTP wildcard match parsing.
CVE-2020-8286	curl 7.41.0 through 7.73.0 is vulnerable to an improper check for certificate revocation due to insufficient verification of the OCSP response.
CVE-2020-8492	Python 2.7 through 2.7.17, 3.5 through 3.5.9, 3.6 through 3.6.10, 3.7 through 3.7.6, and 3.8 through 3.8.1 allows an HTTP server to conduct Regular Expression Denial of Service (ReDoS) attacks against a client because of urllib.request.AbstractBasicAuthHandler catastrophic backtracking.
CVE-2020-8616	A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed

	when processing referrals can, through the use of specially crafted referrals, cause a recursing server to issue a very large number of fetches in an attempt to process the referral. This has at least two potential effects: The performance of the recursing server can potentially be degraded by the additional work required to perform these fetches, and The attacker can exploit this behavior to use the recursing server as a reflector in a reflection attack with a high amplification factor.
CVE-2020-8617	Using a specially-crafted message, an attacker may potentially cause a BIND server to reach an inconsistent state if the attacker knows (or successfully guesses) the name of a TSIG key used by the server. Since BIND, by default, configures a local session key even on servers whose configuration does not otherwise make use of it, almost all current BIND servers are vulnerable. In releases of BIND dating from March 2018 and after, an assertion check in tsig.c detects this inconsistent state and deliberately exits. Prior to the introduction of the check the server would continue operating in an inconsistent state, with potentially harmful results.
CVE-2020-8618	An attacker who is permitted to send zone data to a server via zone transfer can exploit this to intentionally trigger the assertion failure with a specially constructed zone, denying service to clients.
CVE-2020-8619	In ISC BIND9 versions BIND 9.11.14 -> 9.11.19, BIND 9.14.9 -> 9.14.12, BIND 9.16.0 -> 9.16.3, BIND Supported Preview Edition 9.11.14-S1 -> 9.11.19-S1: Unless a nameserver is providing authoritative service for one or more zones and at least one zone contains an empty non-terminal entry containing an asterisk ("*") character, this defect cannot be encountered. A would-be attacker who is allowed to change zone content could theoretically introduce such a record in order to exploit this condition to cause denial of service, though we consider the use of this vector unlikely because any such attack would require a significant privilege level and be easily traceable.
CVE-2020-8620	In BIND 9.15.6 -> 9.16.5, 9.17.0 -> 9.17.3, An attacker who can establish a TCP connection with the server and send data on that connection can exploit this to trigger the assertion failure, causing the server to exit.
CVE-2020-8621	In BIND 9.14.0 -> 9.16.5, 9.17.0 -> 9.17.3, If a server is configured with both QNAME minimization and 'forward first' then an attacker who can send queries to it may be able to trigger the condition that will cause the server to crash. Servers that 'forward only' are not affected.
CVE-2020-8622	In BIND 9.0.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.3-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker on the

	network path for a TSIG-signed request, or operating the server receiving the TSIG-signed request, could send a truncated response to that request, triggering an assertion failure, causing the server to exit. Alternately, an off-path attacker would have to correctly guess when a TSIG-signed request was sent, along with other characteristics of the packet and message, and spoof a truncated response to trigger an assertion failure, causing the server to exit.
CVE-2020-8623	In BIND 9.10.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.10.5-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker that can reach a vulnerable system with a specially crafted query packet can trigger a crash. To be vulnerable, the system must: * be running BIND that was built with "--enable-native-pkcs11" * be signing one or more zones with an RSA key * be able to receive queries from a possible attacker
CVE-2020-8624	In BIND 9.9.12 -> 9.9.13, 9.10.7 -> 9.10.8, 9.11.3 -> 9.11.21, 9.12.1 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.12-S1 -> 9.9.13-S1, 9.11.3-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker who has been granted privileges to change a specific subset of the zone's content could abuse these unintended additional privileges to update other contents of the zone.
CVE-2020-8625	BIND servers are vulnerable if they are running an affected version and are configured to use GSS-TSIG features. In a configuration which uses BIND's default settings the vulnerable code path is not exposed, but a server can be rendered vulnerable by explicitly setting valid values for the tkey-gssapi-keytab or tkey-gssapi-credentialconfiguration options. Although the default configuration is not vulnerable, GSS-TSIG is frequently used in networks where BIND is integrated with Samba, as well as in mixed-server environments that combine BIND servers with Active Directory domain controllers. The most likely outcome of a successful exploitation of the vulnerability is a crash of the named process. However, remote code execution, while unproven, is theoretically possible. Affects: BIND 9.5.0 -> 9.11.27, 9.12.0 -> 9.16.11, and versions BIND 9.11.3-S1 -> 9.11.27-S1 and 9.16.8-S1 -> 9.16.11-S1 of BIND Supported Preview Edition. Also release versions 9.17.0 -> 9.17.1 of the BIND 9.17 development branch
CVE-2020-8694	Insufficient access control in the Linux kernel driver for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2020-8695	Observable discrepancy in the RAPL interface for some Intel(R) Processors may allow a privileged user

	to potentially enable information disclosure via local access.
CVE-2020-8696	Improper removal of sensitive information before storage or transfer in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2020-8698	Improper isolation of shared resources in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2020-8927	A buffer overflow exists in the Brotli library versions prior to 1.0.8 where an attacker controlling the input length of a "one-shot" decompression request to a script can trigger a crash, which happens when copying over chunks of data larger than 2 GiB. It is recommended to update your Brotli library to 1.0.8 or later. If one cannot update, we recommend to use the "streaming" API as opposed to the "one-shot" API, and impose chunk size limits.
CVE-2020-9484	When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter="null" (the default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed.
CVE-2020-9488	Improper validation of certificate with host mismatch in Apache Log4j SMTP appender. This could allow an SMTPS connection to be intercepted by a man-in-the-middle attack which could leak any log messages sent through that appender.
CVE-2020-9490	Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.
CVE-2020-9633	Adobe Flash Player Desktop Runtime 32.0.0.371 and earlier, Adobe Flash Player for Google Chrome 32.0.0.371 and earlier, and Adobe Flash Player for

	Microsoft Edge and Internet Explorer 32.0.0.330 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2020-9746	Adobe Flash Player version 32.0.0.433 (and earlier) are affected by an exploitable NULL pointer dereference vulnerability that could result in a crash and arbitrary code execution. Exploitation of this issue requires an attacker to insert malicious strings in an HTTP response that is by default delivered over TLS/SSL.
CVE-2020-9802	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2020-9803	A memory corruption issue was addressed with improved validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2020-9805	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to universal cross site scripting.
CVE-2020-9806	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2020-9807	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2020-9843	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. Processing maliciously crafted web content may lead to a cross site scripting attack.

CVE-2020-9850	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.5 and iPadOS 13.5, tvOS 13.4.5, watchOS 6.2.5, Safari 13.1.1, iTunes 12.10.7 for Windows, iCloud for Windows 11.2, iCloud for Windows 7.19. A remote attacker may be able to cause arbitrary code execution.
CVE-2020-9862	A command injection issue existed in Web Inspector. This issue was addressed with improved escaping. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Copying a URL from Web Inspector may lead to command injection.
CVE-2020-9893	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.
CVE-2020-9894	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.
CVE-2020-9895	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. A remote attacker may be able to cause unexpected application termination or arbitrary code execution.
CVE-2020-9915	An access issue existed in Content Security Policy. This issue was addressed with improved access restrictions. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may prevent Content Security Policy from being enforced.
CVE-2020-9925	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.6 and iPadOS 13.6, tvOS 13.4.8, watchOS 6.2.8, Safari 13.1.2, iTunes 12.10.8 for Windows, iCloud for Windows 11.3, iCloud for Windows 7.20. Processing maliciously crafted web content may lead to universal cross site scripting.
CVE-2020-9948	A type confusion issue was addressed with improved memory handling. This issue is fixed in Safari 14.0.

	Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2020-9951	A use after free issue was addressed with improved memory management. This issue is fixed in Safari 14.0. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2020-9952	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 14.0 and iPadOS 14.0, tvOS 14.0, watchOS 7.0, Safari 14.0, iCloud for Windows 11.4, iCloud for Windows 7.21. Processing maliciously crafted web content may lead to a cross site scripting attack.
CVE-2020-9983	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in Safari 14.0. Processing maliciously crafted web content may lead to code execution.
CVE-2021-0326	In p2p_copy_client_info of p2p.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution if the target device is performing a Wi-Fi Direct search, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-172937525
CVE-2021-1052	NVIDIA GPU Display Driver for Windows and Linux, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape or IOCTL in which user-mode clients can access legacy privileged APIs, which may lead to denial of service, escalation of privileges, and information disclosure.
CVE-2021-1053	NVIDIA GPU Display Driver for Windows and Linux, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) handler for DxgkDdiEscape or IOCTL in which improper validation of a user pointer may lead to denial of service.
CVE-2021-1056	NVIDIA GPU Display Driver for Linux, all versions, contains a vulnerability in the kernel mode layer (nvidia.ko) in which it does not completely honor operating system file system permissions to provide GPU device-level isolation, which may lead to denial of service or information disclosure.
CVE-2021-1994	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts).

	CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2021-1995	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N).
CVE-2021-1996	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Web Services). Supported versions that are affected are 10.3.6.0.0 and 12.1.3.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle WebLogic Server accessible data. CVSS 3.1 Base Score 2.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N).
CVE-2021-2002	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Replication). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2010	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Client accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Client. CVSS 3.1 Base Score 4.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:L).
CVE-2021-2011	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that

	are affected are 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.1 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2014	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: PAM Auth Plugin). Supported versions that are affected are 5.7.32 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-20177	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2021-20181	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2021-20194	There is a vulnerability in the linux kernel versions higher than 5.2 (if kernel compiled with config params CONFIG_BPF_SYSCALL=y , CONFIG_BPF=y , CONFIG_CGROUPS=y , CONFIG_CGROUP_BPF=y , CONFIG_HARDENED_USERCOPY not set, and BPF hook to getsockopt is registered). As result of BPF execution, the local user can trigger bug in __cgroup_bpf_run_filter_getsockopt() function that can lead to heap overflow (because of non-hardened usercopy). The impact of attack could be deny of service or possibly privileges escalation.
CVE-2021-2021	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability

	impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2022	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-20239	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2021-2024	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2031	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2032	Vulnerability in the MySQL Server product of Oracle MySQL (component: Information Schema). Supported versions that are affected are 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.1 Base Score 4.3 (Confidentiality

	impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).
CVE-2021-2033	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core Components). Supported versions that are affected are 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows low privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle WebLogic Server. CVSS 3.1 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L).
CVE-2021-20353	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 194882.
CVE-2021-2036	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2038	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Components Services). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2046	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized

	ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).
CVE-2021-2047	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core Components). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2021-2048	Vulnerability in the MySQL Server product of Oracle MySQL (component: InnoDB). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.1 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2021-2056	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2058	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Locking). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVE-2021-2060	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.50 and prior, 5.7.32 and prior and 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2061	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2064	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core Components). The supported version that is affected is 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2021-2065	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2070	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this

	vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2072	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2075	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Samples). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2021-2076	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2081	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2087	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions

	that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2088	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-2108	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Core Components). The supported version that is affected is 12.1.3.0.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via IIOP, T3 to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 9.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2021-2109	Vulnerability in the Oracle WebLogic Server product of Oracle Fusion Middleware (component: Console). Supported versions that are affected are 10.3.6.0.0, 12.1.3.0.0, 12.2.1.3.0, 12.2.1.4.0 and 14.1.1.0.0. Easily exploitable vulnerability allows high privileged attacker with network access via HTTP to compromise Oracle WebLogic Server. Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2021-21106	Use after free in autofill in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21107	Use after free in drag and drop in Google Chrome on Linux prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.

CVE-2021-21108	Use after free in media in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21109	Use after free in payments in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21110	Use after free in safe browsing in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21111	Insufficient policy enforcement in WebUI in Google Chrome prior to 87.0.4280.141 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2021-21112	Use after free in Blink in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21113	Heap buffer overflow in Skia in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21114	Use after free in audio in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21115	User after free in safe browsing in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21116	Heap buffer overflow in audio in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21117	Insufficient policy enforcement in Cryptohome in Google Chrome prior to 88.0.4324.96 allowed a local attacker to perform OS-level privilege escalation via a crafted file.
CVE-2021-21118	Insufficient data validation in V8 in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2021-21119	Use after free in Media in Google Chrome prior to 88.0.4324.96 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21120	Use after free in WebSQL in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2021-21121	Use after free in Omnibox in Google Chrome on Linux prior to 88.0.4324.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21122	Use after free in Blink in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21123	Insufficient data validation in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.
CVE-2021-21124	Potential user after free in Speech Recognizer in Google Chrome on Android prior to 88.0.4324.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21125	Insufficient policy enforcement in File System API in Google Chrome on Windows prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.
CVE-2021-21126	Insufficient policy enforcement in extensions in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass site isolation via a crafted Chrome Extension.
CVE-2021-21127	Insufficient policy enforcement in extensions in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass content security policy via a crafted Chrome Extension.
CVE-2021-21128	Heap buffer overflow in Blink in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21129	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.
CVE-2021-21130	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.
CVE-2021-21131	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.
CVE-2021-21132	Inappropriate implementation in DevTools in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2021-21133	Insufficient policy enforcement in Downloads in Google Chrome prior to 88.0.4324.96 allowed an attacker who

	convinced a user to download files to bypass navigation restrictions via a crafted HTML page.
CVE-2021-21134	Incorrect security UI in Page Info in Google Chrome on iOS prior to 88.0.4324.96 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2021-21135	Inappropriate implementation in Performance API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-21136	Insufficient policy enforcement in WebView in Google Chrome on Android prior to 88.0.4324.96 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-21137	Inappropriate implementation in DevTools in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to obtain potentially sensitive information from disk via a crafted HTML page.
CVE-2021-21138	Use after free in DevTools in Google Chrome prior to 88.0.4324.96 allowed a local attacker to potentially perform a sandbox escape via a crafted file.
CVE-2021-21139	Inappropriate implementation in iframe sandbox in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2021-21140	Uninitialized use in USB in Google Chrome prior to 88.0.4324.96 allowed a local attacker to potentially perform out of bounds memory access via via a USB device.
CVE-2021-21141	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass file extension policy via a crafted HTML page.
CVE-2021-21142	Use after free in Payments in Google Chrome on Mac prior to 88.0.4324.146 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21143	Heap buffer overflow in Extensions in Google Chrome prior to 88.0.4324.146 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2021-21144	Heap buffer overflow in Tab Groups in Google Chrome prior to 88.0.4324.146 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2021-21145	Use after free in Fonts in Google Chrome prior to 88.0.4324.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2021-21146	Use after free in Navigation in Google Chrome prior to 88.0.4324.146 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21147	Inappropriate implementation in Skia in Google Chrome prior to 88.0.4324.146 allowed a local attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2021-21148	Heap buffer overflow in V8 in Google Chrome prior to 88.0.4324.150 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21149	Stack buffer overflow in Data Transfer in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.
CVE-2021-21150	Use after free in Downloads in Google Chrome on Windows prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21151	Use after free in Payments in Google Chrome prior to 88.0.4324.182 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21152	Heap buffer overflow in Media in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21153	Stack buffer overflow in GPU Process in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2021-21154	Heap buffer overflow in Tab Strip in Google Chrome prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21155	Heap buffer overflow in Tab Strip in Google Chrome on Windows prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21156	Heap buffer overflow in V8 in Google Chrome prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted script.
CVE-2021-21157	Use after free in Web Sockets in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21159	Heap buffer overflow in TabStrip in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to

	potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21160	Heap buffer overflow in WebAudio in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21161	Heap buffer overflow in TabStrip in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21162	Use after free in WebRTC in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21163	Insufficient data validation in Reader Mode in Google Chrome on iOS prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page and a malicious server.
CVE-2021-21165	Data race in audio in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21166	Data race in audio in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21167	Use after free in bookmarks in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21168	Insufficient policy enforcement in appcache in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2021-21169	Out of bounds memory access in V8 in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2021-21170	Incorrect security UI in Loader in Google Chrome prior to 89.0.4389.72 allowed a remote attacker who had compromised the renderer process to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2021-21171	Incorrect security UI in TabStrip and Navigation in Google Chrome on Android prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2021-21172	Insufficient policy enforcement in File System API in Google Chrome on Windows prior to 89.0.4389.72 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.

CVE-2021-21173	Side-channel information leakage in Network Internals in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-21174	Inappropriate implementation in Referrer in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2021-21175	Inappropriate implementation in Site isolation in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-21176	Inappropriate implementation in full screen mode in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2021-21177	Insufficient policy enforcement in Autofill in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2021-21178	Inappropriate implementation in Compositing in Google Chrome on Linux and Windows prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2021-21179	Use after free in Network Internals in Google Chrome on Linux prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21180	Use after free in tab search in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21181	Side-channel information leakage in autofill in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2021-21182	Insufficient policy enforcement in navigations in Google Chrome prior to 89.0.4389.72 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.
CVE-2021-21183	Inappropriate implementation in performance APIs in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-21184	Inappropriate implementation in performance APIs in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-21185	Insufficient policy enforcement in extensions in Google Chrome prior to 89.0.4389.72 allowed an attacker who convinced a user to install a malicious extension

	to obtain sensitive information via a crafted Chrome Extension.
CVE-2021-21186	Insufficient policy enforcement in QR scanning in Google Chrome on iOS prior to 89.0.4389.72 allowed an attacker who convinced the user to scan a QR code to bypass navigation restrictions via a crafted QR code.
CVE-2021-21187	Insufficient data validation in URL formatting in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2021-21188	Use after free in Blink in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21189	Insufficient policy enforcement in payments in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2021-21190	Uninitialized data in PDFium in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.
CVE-2021-2122	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DDL). Supported versions that are affected are 8.0.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2021-21261	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. A bug was discovered in the \`flatpak-portal\` service that can allow sandboxed applications to execute arbitrary code on the host system (a sandbox escape). This sandbox-escape bug is present in versions from 0.11.4 and before fixed versions 1.8.5 and 1.10.0. The Flatpak portal D-Bus service (\`flatpak-portal\`, also known by its D-Bus service name \`org.freedesktop.portal.Flatpak\`) allows apps in a Flatpak sandbox to launch their own subprocesses in a new sandbox instance, either with the same security settings as the caller or with more restrictive security settings. For example, this is used in Flatpak-packaged web browsers such as Chromium to launch subprocesses that will process untrusted web content, and give those subprocesses a more restrictive sandbox than the browser itself. In vulnerable versions, the Flatpak portal service passes caller-specified environment variables to non-sandboxed

	processes on the host system, and in particular to the `flatpak run` command that is used to launch the new sandbox instance. A malicious or compromised Flatpak app could set environment variables that are trusted by the `flatpak run` command, and use them to execute arbitrary code that is not in a sandbox. As a workaround, this vulnerability can be mitigated by preventing the `flatpak-portal` service from starting, but that mitigation will prevent many Flatpak apps from working correctly. This is fixed in versions 1.8.5 and 1.10.0.
CVE-2021-21300	Git is an open-source distributed revision control system. In affected versions of Git a specially crafted repository that contains symbolic links as well as files using a clean/smudge filter such as Git LFS, may cause just-checked out script to be executed while cloning onto a case-insensitive file system such as NTFS, HFS + or APFS (i.e. the default file systems on Windows and macOS). Note that clean/smudge filters have to be configured for that. Git for Windows configures Git LFS by default, and is therefore vulnerable. The problem has been patched in the versions published on Tuesday, March 9th, 2021. As a workaound, if symbolic link support is disabled in Git (e.g. via `git config --global core.symlinks false`), the described attack won't work. Likewise, if no clean/smudge filters such as Git LFS are configured globally (i.e. _before_ cloning), the attack is foiled. As always, it is best to avoid cloning repositories from untrusted sources. The earliest impacted version is 2.14.2. The fix versions are: 2.30.1, 2.29.3, 2.28.1, 2.27.1, 2.26.3, 2.25.5, 2.24.4, 2.23.4, 2.22.5, 2.21.4, 2.20.5, 2.19.6, 2.18.5, 2.17.62.17.6.
CVE-2021-21334	In containerd (an industry-standard container runtime) before versions 1.3.10 and 1.4.4, containers launched through containerd's CRI implementation (through Kubernetes, crictl, or any other pod/container client that uses the containerd CRI service) that share the same image may receive incorrect environment variables, including values that are defined for other containers. If the affected containers have different security contexts, this may allow sensitive information to be unintentionally shared. If you are not using containerd's CRI implementation (through one of the mechanisms described above), you are not vulnerable to this issue. If you are not launching multiple containers or Kubernetes pods from the same image which have different environment variables, you are not vulnerable to this issue. If you are not launching multiple containers or Kubernetes pods from the same image in rapid succession, you have reduced likelihood of being vulnerable to this issue This vulnerability has been fixed

	in containerd 1.3.10 and containerd 1.4.4. Users should update to these versions.
CVE-2021-21602	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier allows reading arbitrary files using the file browser for workspaces and archived artifacts by following symlinks.
CVE-2021-21603	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not escape notification bar response contents, resulting in a cross-site scripting (XSS) vulnerability.
CVE-2021-21604	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier allows attackers with permission to create or configure various objects to inject crafted content into Old Data Monitor that results in the instantiation of potentially unsafe objects once discarded by an administrator.
CVE-2021-21605	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier allows users with Agent/Configure permission to choose agent names that cause Jenkins to override the global `config.xml` file.
CVE-2021-21606	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier improperly validates the format of a provided fingerprint ID when checking for its existence allowing an attacker to check for the existence of XML files with a short path.
CVE-2021-21607	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not limit sizes provided as query parameters to graph-rendering URLs, allowing attackers to request crafted URLs that use all available memory in Jenkins, potentially leading to out of memory errors.
CVE-2021-21608	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not escape button labels in the Jenkins UI, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers with the ability to control button labels.
CVE-2021-21609	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not correctly match requested URLs to the list of always accessible paths, allowing attackers without Overall/Read permission to access some URLs as if they did have Overall/Read permission.
CVE-2021-21610	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not implement any restrictions for the URL rendering a formatted preview of markup passed as a query parameter, resulting in a reflected cross-site scripting (XSS) vulnerability if the configured markup formatter does not prohibit unsafe elements (JavaScript) in markup.
CVE-2021-21611	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not escape display names and IDs of item types shown on the New Item page, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to specify display names or IDs of item types.

CVE-2021-21615	Jenkins 2.275 and LTS 2.263.2 allows reading arbitrary files using the file browser for workspaces and archived artifacts due to a time-of-check to time-of-use (TOCTOU) race condition.
CVE-2021-22132	Elasticsearch versions 7.7.0 to 7.10.1 contain an information disclosure flaw in the async search API. Users who execute an async search will improperly store the HTTP headers. An Elasticsearch user with the ability to read the .tasks index could obtain sensitive request headers of other users in the cluster. This issue is fixed in Elasticsearch 7.10.2
CVE-2021-23239	The sudoedit personality of Sudo before 1.9.5 may allow a local unprivileged user to perform arbitrary directory-existence tests by winning a sudo_edit.c race condition in replacing a user-controlled directory by a symlink to an arbitrary path.
CVE-2021-23336	The package python/cpython from 0 and before 3.6.13, from 3.7.0 and before 3.7.10, from 3.8.0 and before 3.8.8, from 3.9.0 and before 3.9.2 are vulnerable to Web Cache Poisoning via urllib.parse.parse_qsl and urllib.parse.parse_qs by using a vector called parameter cloaking. When the attacker can separate query parameters using a semicolon (;), they can cause a difference in the interpretation of the request between the proxy (running with default configuration) and the server. This can result in malicious requests being cached as completely safe ones, as the proxy would usually not see the semicolon as a separator, and therefore would not include it in a cache key of an unkeyed parameter.
CVE-2021-23840	Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).
CVE-2021-23841	The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate.

	However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).
CVE-2021-23953	If a user clicked into a specifically crafted PDF, the PDF reader could be confused into leaking cross-origin information, when said information is served as chunked data. This vulnerability affects Firefox < 85, Thunderbird < 78.7, and Firefox ESR < 78.7.
CVE-2021-23954	Using the new logical assignment operators in a JavaScript switch statement could have caused a type confusion, leading to a memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 85, Thunderbird < 78.7, and Firefox ESR < 78.7.
CVE-2021-23955	The browser could have been confused into transferring a pointer lock state into another tab, which could have lead to clickjacking attacks. This vulnerability affects Firefox < 85.
CVE-2021-23956	An ambiguous file picker design could have confused users who intended to select and upload a single file into uploading a whole directory. This was addressed by adding a new prompt. This vulnerability affects Firefox < 85.
CVE-2021-23958	The browser could have been confused into transferring a screen sharing state into another tab, which would leak unintended information. This vulnerability affects Firefox < 85.
CVE-2021-23960	Performing garbage collection on re-declared JavaScript variables resulted in a user-after-poison, and a potentially exploitable crash. This vulnerability affects Firefox < 85, Thunderbird < 78.7, and Firefox ESR < 78.7.
CVE-2021-23961	Further techniques that built on the slipstream research combined with a malicious webpage could have exposed both an internal network's hosts as well as

	services running on the user's local machine. This vulnerability affects Firefox < 85.
CVE-2021-23962	Incorrect use of the '<RowCountChanged>' method could have led to a user-after-poison and a potentially exploitable crash. This vulnerability affects Firefox < 85.
CVE-2021-23963	When sharing geolocation during an active WebRTC share, Firefox could have reset the webRTC sharing state in the user interface, leading to loss of control over the currently granted permission. This vulnerability affects Firefox < 85.
CVE-2021-23964	Mozilla developers reported memory safety bugs present in Firefox 84 and Firefox ESR 78.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 85, Thunderbird < 78.7, and Firefox ESR < 78.7.
CVE-2021-23965	Mozilla developers reported memory safety bugs present in Firefox 84. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 85.
CVE-2021-23968	If Content Security Policy blocked frame navigation, the full destination of a redirect served in the frame was reported in the violation report; as opposed to the original frame URI. This could be used to leak sensitive information contained in such URIs. This vulnerability affects Firefox < 86, Thunderbird < 78.8, and Firefox ESR < 78.8.
CVE-2021-23969	As specified in the W3C Content Security Policy draft, when creating a violation report, "User agents need to ensure that the source file is the URL requested by the page, pre-redirects. If that’s not possible, user agents need to strip the URL down to an origin to avoid unintentional leakage." Under certain types of redirects, Firefox incorrectly set the source file to be the destination of the redirects. This was fixed to be the redirect destination's origin. This vulnerability affects Firefox < 86, Thunderbird < 78.8, and Firefox ESR < 78.8.
CVE-2021-23970	Context-specific code was included in a shared jump table; resulting in assertions being triggered in multithreaded wasm code. This vulnerability affects Firefox < 86.
CVE-2021-23971	When processing a redirect with a conflicting Referrer-Policy, Firefox would have adopted the redirect's Referrer-Policy. This would have potentially resulted in more information than intended by the original origin

	being provided to the destination of the redirect. This vulnerability affects Firefox < 86.
CVE-2021-23972	One phishing tactic on the web is to provide a link with HTTP Auth. For example 'https://www.phishingtarget.com@evil.com'. To mitigate this type of attack, Firefox will display a warning dialog; however, this warning dialog would not have been displayed if evil.com used a redirect that was cached by the browser. This vulnerability affects Firefox < 86.
CVE-2021-23973	When trying to load a cross-origin resource in an audio/video context a decoding error may have resulted, and the content of that error may have revealed information about the resource. This vulnerability affects Firefox < 86, Thunderbird < 78.8, and Firefox ESR < 78.8.
CVE-2021-23974	The DOMParser API did not properly process '<noscript>' elements for escaping. This could be used as an mXSS vector to bypass an HTML Sanitizer. This vulnerability affects Firefox < 86.
CVE-2021-23975	The developer page about:memory has a Measure function for exploring what object types the browser has allocated and their sizes. When this function was invoked we incorrectly called the sizeof function, instead of using the API method that checks for invalid pointers. This vulnerability affects Firefox < 86.
CVE-2021-23978	Mozilla developers reported memory safety bugs present in Firefox 85 and Firefox ESR 78.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 86, Thunderbird < 78.8, and Firefox ESR < 78.8.
CVE-2021-23979	Mozilla developers reported memory safety bugs present in Firefox 85. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 86.
CVE-2021-24031	In the Zstandard command-line utility prior to v1.4.1, output files were created with default permissions. Correct file permissions (matching the input) would only be set at completion time. Output files could therefore be readable or writable to unintended parties.
CVE-2021-24032	Beginning in v1.4.1 and prior to v1.4.9, due to an incomplete fix for CVE-2021-24031, the Zstandard command-line utility created output files with default permissions and restricted those permissions immediately afterwards. Output files could therefore momentarily be readable or writable to unintended parties.

CVE-2021-25289	An issue was discovered in Pillow before 8.1.1. TiffDecode has a heap-based buffer overflow when decoding crafted YCbCr files because of certain interpretation conflicts with LibTIFF in RGBA mode. NOTE: this issue exists because of an incomplete fix for CVE-2020-35654.
CVE-2021-25290	An issue was discovered in Pillow before 8.1.1. In TiffDecode.c, there is a negative-offset memcpy with an invalid size.
CVE-2021-25291	An issue was discovered in Pillow before 8.1.1. In TiffDecode.c, there is an out-of-bounds read in TiffreadRGBATile via invalid tile boundaries.
CVE-2021-25292	An issue was discovered in Pillow before 8.1.1. The PDF parser allows a regular expression DoS (ReDoS) attack via a crafted PDF file because of a catastrophic backtracking regex.
CVE-2021-25293	An issue was discovered in Pillow before 8.1.1. There is an out-of-bounds read in SGIRleDecode.c.
CVE-2021-26708	A local privilege escalation was discovered in the Linux kernel before 5.10.13. Multiple race conditions in the AF_VSOCK implementation are caused by wrong locking in net/vmw_vsock/af_vsock.c. The race conditions were implicitly introduced in the commits that added VSOCK multi-transport support.
CVE-2021-26937	encoding.c in GNU Screen through 4.8.0 allows remote attackers to cause a denial of service (invalid write access and application crash) or possibly have unspecified other impact via a crafted UTF-8 character sequence.
CVE-2021-27135	xterm before Patch #366 allows remote attackers to execute arbitrary code or cause a denial of service (segmentation fault) via a crafted UTF-8 combining character sequence.
CVE-2021-27212	In OpenLDAP through 2.4.57 and 2.5.x through 2.5.1alpha, an assertion failure in slapd can occur in the issuerAndThisUpdateCheck function via a crafted packet, resulting in a denial of service (daemon exit) via a short timestamp. This is related to schema_init.c and checkTime.
CVE-2021-27218	An issue was discovered in GNOME GLib before 2.66.7 and 2.67.x before 2.67.4. If g_byte_array_new_take() was called with a buffer of 4GB or more on a 64-bit platform, the length would be truncated modulo 2**32, causing unintended length truncation.
CVE-2021-27219	An issue was discovered in GNOME GLib before 2.66.6 and 2.67.x before 2.67.3. The function g_bytes_new has an integer overflow on 64-bit platforms due to an implicit cast from 64 bits to 32 bits. The overflow could potentially lead to memory corruption.

CVE-2021-27803	A vulnerability was discovered in how p2p/p2p_pd.c in wpa_supplicant before 2.10 processes P2P (Wi-Fi Direct) provision discovery requests. It could result in denial of service or other impact (potentially execution of arbitrary code), for an attacker within radio range.
CVE-2021-27921	Pillow before 8.1.1 allows attackers to cause a denial of service (memory consumption) because the reported size of a contained image is not properly checked for a BLP container, and thus an attempted memory allocation can be very large.
CVE-2021-27922	Pillow before 8.1.1 allows attackers to cause a denial of service (memory consumption) because the reported size of a contained image is not properly checked for an ICNS container, and thus an attempted memory allocation can be very large.
CVE-2021-28041	ssh-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.
CVE-2021-28153	An issue was discovered in GNOME GLib before 2.66.8. When g_file_replace() is used with G_FILE_CREATE_REPLACE_DESTINATION to replace a path that is a dangling symlink, it incorrectly also creates the target of the symlink as an empty file, which could conceivably have security relevance if the symlink is attacker-controlled. (If the path is a symlink to a file that already exists, then the contents of that file correctly remain unchanged.)
CVE-2021-3139	In Open-iSCSI tcmu-runner 1.3.x, 1.4.x, and 1.5.x through 1.5.2, xcopy_locate_udev in tcmur_cmd_handler.c lacks a check for transport-layer restrictions, allowing remote attackers to read or write files via directory traversal in an XCOPY request. For example, an attack can occur over a network if the attacker has access to one iSCSI LUN. NOTE: relative to CVE-2020-28374, this is a similar mistake in a different algorithm.
CVE-2021-3156	Sudo before 1.9.5p2 contains an off-by-one error that can result in a heap-based buffer overflow, which allows privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character.
CVE-2021-3177	Python 3.x through 3.9.1 has a buffer overflow in PyCArg_repr in _ctypes/callproc.c, which may lead to remote code execution in certain Python applications that accept floating-point numbers as untrusted input, as demonstrated by a 1e300 argument to c_double.from_param. This occurs because sprintf is used unsafely.

CVE-2021-3178	** DISPUTED ** fs/nfsd/nfs3xdr.c in the Linux kernel through 5.10.8, when there is an NFS export of a subdirectory of a filesystem, allows remote attackers to traverse to other parts of the filesystem via READDIRPLUS. NOTE: some parties argue that such a subdirectory export is not intended to prevent this attack; see also the exports(5) no_subtree_check default behavior.
CVE-2021-3181	rfc822.c in Mutt through 2.0.4 allows remote attackers to cause a denial of service (mailbox unavailability) by sending email messages with sequences of semicolon characters in RFC822 address fields (aka terminators of empty groups). A small email message from the attacker can cause large memory consumption, and the victim may then be unable to see email messages from other persons.
CVE-2021-3281	In Django 2.2 before 2.2.18, 3.0 before 3.0.12, and 3.1 before 3.1.6, the django.utils.archive.extract method (used by "startapp --template" and "startproject --template") allows directory traversal via an archive with absolute paths or relative paths with dot segments.
CVE-2021-3347	An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault handling, allowing local users to execute code in the kernel, aka CID-34b1a1ce1458.
CVE-2021-3393	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

5.2 Passed rules - Network Reachability-1.1

Rule	Description
Recognized port with listener reachable from a Peered VPC	A recognized port is reachable from a Peered VPC with a service listening
Recognized port with listener reachable from a Virtual Private Gateway	A recognized port is reachable from a Virtual Private Gateway with a service listening
Recognized port with listener reachable from internet	A recognized port is reachable from the internet with a service listening
Recognized port with no listener reachable from a Peered VPC	On this instance, recognized port(s) are reachable from a Peered VPC with no process listening on the port.
Recognized port with no listener reachable from a Virtual Private Gateway	On this instance, recognized port(s) are reachable from a Virtual Private Gateway with no process listening on the port.
Unrecognized port with listener reachable from a Peered VPC	An unrecognized port is reachable from a Peered VPC with a service listening

Unrecognized port with listener reachable from a Virtual Private Gateway	An unrecognized port is reachable from a Virtual Private Gateway with a service listening
Unrecognized port with listener reachable from internet	An unrecognized port is reachable from the internet with a service listening

5.3 Passed rules - Security Best Practices-1.0

Rule	Description
Configure Password Complexity	This rule helps determine whether a password complexity mechanism is configured on your EC2 instances.
Configure Password Maximum Age	This rule helps determine whether maximum age for passwords is configured on your EC2 instances.
Configure Password Minimum Length	This rule helps determine whether minimum length for passwords is configured on your EC2 instances.
Configure permissions for system directories	This rule checks permissions on system directories that contain binaries and system configuration information to make sure that only the root user (a user who logs in by using root account credentials) has write permissions for these directories.
Disable Password Authentication Over SSH	This rule helps determine whether your EC2 instances are configured to support password authentication over the SSH protocol.
Disable root login over SSH	This rule helps determine whether the SSH daemon is configured to permit logging in to your EC2 instance as root.
Disable root login over SSH with a command authenticated by public key	This rule helps determine whether the SSH daemon is configured to permit logging in to your EC2 instance as root using a command authenticated by a public key.
Enable ASLR	This rule helps determine whether address space layout randomization (ASLR) is enabled on the operating systems of the EC2 instances in your assessment target.
Enable DEP	This rule helps determine whether Data Execution Prevention (DEP) is enabled on the operating systems of the EC2 instances in your assessment target.
Support SSH Version 2 Only	This rule helps determine whether your EC2 instances are configured to support SSH protocol version 1.0.