Amazon Inspector - Assessment Report

Full Report

Report generated on 2017-10-29 at 23:47:38 UTC

Assessment Template: MyFirstTemplateLinux2

Assessment Run start: 2017-10-29 at 22:14:54 UTC
Assessment Run end: 2017-10-29 at 22:31:27 UTC

Section 1: Executive Summary

This is an Inspector assessment report for an assessment started on 2017-10-29 22:14:54 UTC for assessment template 'MyFirstTemplateLinux2'. The assessment target included 1 instances, and was tested against 1 Rules Packages.

The assessment target is defined using the following EC2 tags

Key	Value
Name	InspectorEC2InstanceLinux

The following Rules Packages were assessed. A total of 46 findings were created, with the following distribution by severity:

Rules Package	High	Medium	Low	Informational
Common Vulnerabilities and Exposures-1.1	25	19	2	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: 1

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

2.2: Assessment Target - MyFirstTemplateLinux2

2.2.1: EC2 Tags:

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

Key	Value
Name	InspectorEC2InstanceLinux

2.2.2: Instances - Count 1

Instance ID
i-035c60a4c31f51e7b

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

Rule	Severity	Failed
CVE-2016-0634	High	1
CVE-2016-10009	High	1
CVE-2016-10011	Medium	1
CVE-2016-10012	High	1
CVE-2016-6210	Medium	1
CVE-2016-6515	High	1
CVE-2016-7543	High	1
CVE-2016-9401	Medium	1
CVE-2017-1000099	Medium	1
CVE-2017-1000100	Low	1
CVE-2017-1000101	Medium	1
CVE-2017-1000111	High	1
CVE-2017-1000112	High	1
CVE-2017-1000364	High	1
CVE-2017-1000365	High	1
CVE-2017-1000370	High	1
CVE-2017-1000371	High	1
CVE-2017-1000377	Medium	1
CVE-2017-11473	High	1
CVE-2017-12134	High	1
CVE-2017-14497	High	1
CVE-2017-2616	Medium	1
CVE-2017-2671	Medium	1
CVE-2017-5967	Medium	1

CVE-2017-6451	Medium	1
CVE-2017-6458	High	1
CVE-2017-6462	Medium	1
CVE-2017-6463	Medium	1
CVE-2017-6464	Medium	1
CVE-2017-7187	High	1
CVE-2017-7308	High	1
CVE-2017-7407	Medium	1
CVE-2017-7488	Medium	1
CVE-2017-7533	High	1
CVE-2017-7542	Medium	1
CVE-2017-7558	Low	1
CVE-2017-7616	Medium	1
CVE-2017-7618	High	1
CVE-2017-8831	High	1
CVE-2017-8890	High	1
CVE-2017-9059	Medium	1
CVE-2017-9074	High	1
CVE-2017-9075	High	1
CVE-2017-9076	High	1
CVE-2017-9077	High	1
CVE-2017-9242	Medium	1

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

CVE-2016-0634

Severity
High

Description
The expansion of '\h' in the prompt string in bash 4.3 allows remote authenticated users to execute arbitrary code via shell metacharacters placed in 'hostname' of a machine.

Recommendation
Use your Operating System's update feature to update package bash, bash-0:4.1.2-15.24.amzn1, bash-0:4.1.2-15.el6_5.2, bash-0:4.1.2-40.el6, bash-0:4.2.46-12.34.amzn1, bash-0:4.2.46-19.el7, bash-0:4.2.46-20.36.amzn1, bash-0:4.2.46-20.el7_2, bash-0:4.3-7ubuntu1.5, bash-0:4.3-7ubuntu1.6. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0634

Failed Instances
i-035c60a4c31f51e7b

CVE-2016-10009

Severity
High

Description

Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.

Recommendation
Use your Operating System's update feature to update package openssh, openssh-0:6.2p2-8.44.amzn1, openssh-0:6.6.1p1-22.el7, openssh-0:6.6.1p1-23.59.amzn1, openssh-0:6.6.1p1-31.el7, openssh-0:6.6.1p1-33.66.amzn1, openssh-clients-0:6.2p2-8.44.amzn1, openssh-clients-0:6.6.1p1-22.el7, openssh-clients-0:6.6.1p1-23.59.amzn1, openssh-clients-0:6.6.1p1-31.el7, openssh-clients-0:6.6.1p1-33.66.amzn1, openssh-server-0:6.2p2-8.44.amzn1, openssh-server-0:6.6.1p1-22.el7, openssh-server-0:6.6.1p1-23.59.amzn1, openssh-server-0:6.6.1p1-31.el7, openssh-server-0:6.6.1p1-33.66.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10009

Failed Instances
i-035c60a4c31f51e7b

CVE-2016-10011

Severity
Medium

Description
authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.

Recommendation
Use your Operating System's update feature to update package openssh, openssh-0:6.2p2-8.44.amzn1, openssh-0:6.6.1p1-22.el7, openssh-0:6.6.1p1-23.59.amzn1, openssh-0:6.6.1p1-31.el7, openssh-0:6.6.1p1-33.66.amzn1, openssh-clients-0:6.2p2-8.44.amzn1, openssh-clients-0:6.6.1p1-22.el7, openssh-clients-0:6.6.1p1-23.59.amzn1, openssh-clients-0:6.6.1p1-31.el7, openssh-clients-0:6.6.1p1-33.66.amzn1, openssh-server-0:6.2p2-8.44.amzn1, openssh-server-0:6.6.1p1-22.el7, openssh-server-0:6.6.1p1-23.59.amzn1, openssh-server-0:6.6.1p1-31.el7, openssh-server-0:6.6.1p1-33.66.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10011

Failed Instances
i-035c60a4c31f51e7b

CVE-2016-10012

Severity
High

Description
The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.

Recommendation
Use your Operating System's update feature to update package openssh, openssh-0:6.2p2-8.44.amzn1, openssh-0:6.6.1p1-22.el7, openssh-0:6.6.1p1-23.59.amzn1, openssh-0:6.6.1p1-31.el7, openssh-0:6.6.1p1-33.66.amzn1, openssh-clients-0:6.2p2-8.44.amzn1, openssh-clients-0:6.6.1p1-22.el7, openssh-clients-0:6.6.1p1-23.59.amzn1, openssh-clients-0:6.6.1p1-31.el7, openssh-clients-0:6.6.1p1-33.66.amzn1, openssh-server-0:6.2p2-8.44.amzn1, openssh-server-0:6.6.1p1-22.el7, openssh-server-0:6.6.1p1-23.59.amzn1, openssh-server-0:6.6.1p1-31.el7, openssh-server-0:6.6.1p1-33.66.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-10012

Failed Instances
i-035c60a4c31f51e7b

CVE-2016-6210

Severity
Medium

Description
sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.

Recommendation
Use your Operating System's update feature to update package openssh, openssh-0:5.3p1-118.1.el6_8, openssh-0:5.3p1-122.el6, openssh-0:5.3p1-94.el6, openssh-0:6.2p2-8.44.amzn1, openssh-0:6.6.1p1-22.el7, openssh-0:6.6.1p1-23.59.amzn1, openssh-0:6.6.1p1-31.el7, openssh-0:6.6.1p1-33.66.amzn1, openssh-clients-0:5.3p1-118.1.el6_8, openssh-clients-0:5.3p1-122.el6, openssh-clients-0:5.3p1-94.el6, openssh-clients-0:6.2p2-8.44.amzn1, openssh-clients-0:6.6.1p1-22.el7, openssh-clients-0:6.6.1p1-23.59.amzn1, openssh-clients-0:6.6.1p1-31.el7, openssh-clients-0:6.6.1p1-33.66.amzn1, openssh-server, openssh-server-0:5.3p1-118.1.el6_8, openssh-server-0:5.3p1-122.el6, openssh-server-0:5.3p1-94.el6, openssh-server-0:6.2p2-8.44.amzn1, openssh-server-0:6.6.1p1-22.el7, openssh-server-0:6.6.1p1-23.59.amzn1, openssh-server-0:6.6.1p1-31.el7, openssh-server-0:6.6.1p1-33.66.amzn1, openssh-server-1:6.6p1-2ubuntu2. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6210

Failed Instances
i-035c60a4c31f51e7b

CVE-2016-6515

Severity
High

Description
The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.

Recommendation
Use your Operating System's update feature to update package openssh, openssh-0:6.2p2-8.44.amzn1, openssh-0:6.6.1p1-22.el7, openssh-0:6.6.1p1-23.59.amzn1, openssh-0:6.6.1p1-31.el7, openssh-0:6.6.1p1-33.66.amzn1, openssh-clients-0:6.2p2-8.44.amzn1, openssh-clients-0:6.6.1p1-22.el7, openssh-clients-0:6.6.1p1-23.59.amzn1, openssh-clients-0:6.6.1p1-31.el7, openssh-clients-0:6.6.1p1-33.66.amzn1, openssh-server, openssh-server-0:6.2p2-8.44.amzn1, openssh-server-0:6.6.1p1-22.el7, openssh-server-0:6.6.1p1-23.59.amzn1, openssh-server-0:6.6.1p1-31.el7, openssh-server-0:6.6.1p1-33.66.amzn1, openssh-server-1:6.6p1-2ubuntu2. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6515

Failed Instances
i-035c60a4c31f51e7b

CVE-2016-7543

Severity
High

Description
Bash before 4.4 allows local users to execute arbitrary commands with root privileges via crafted SHELLOPTS and PS4 environment variables.

Recommendation
Use your Operating System's update feature to update package bash, bash-0:4.1.2-15.24.amzn1, bash-0:4.1.2-15.el6_5.2, bash-0:4.1.2-40.el6, bash-0:4.2.46-12.34.amzn1, bash-0:4.2.46-19.el7, bash-0:4.2.46-20.36.amzn1, bash-0:4.2.46-20.el7_2, bash-0:4.3-7ubuntu1.5, bash-0:4.3-7ubuntu1.6. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-7543

Failed Instances
i-035c60a4c31f51e7b

CVE-2016-9401

Severity
Medium

Description
popd in bash might allow local users to bypass the restricted shell and cause a use-after-free via a crafted address.

Recommendation
Use your Operating System's update feature to update package bash, bash-0:4.1.2-15.24.amzn1, bash-0:4.1.2-15.el6_5.2, bash-0:4.1.2-40.el6, bash-0:4.2.46-12.34.amzn1, bash-0:4.2.46-19.el7, bash-0:4.2.46-20.36.amzn1, bash-0:4.2.46-20.el7_2, bash-0:4.3-7ubuntu1.5, bash-0:4.3-7ubuntu1.6. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9401

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-1000099

Severity
Medium

Description
When asking to get a file from a file:// URL, libcurl provides a feature that outputs meta-data about the file using HTTP-like headers.The code doing this would send the wrong buffer to the user (stdout or the application's provide callback), which could lead to other private data from the heap to get inadvertently displayed. The wrong bufferwas an uninitialized memory area allocated on the heap and if it turned out to not contain any zero byte, it would continue and displaythe data following that buffer in memory.

Recommendation
Use your Operating System's update feature to update package curl, curl-0:7.40.0-3.52.amzn1, curl-0:7.40.0-8.54.amzn1, curl-0:7.51.0-4.73.amzn1, curl-0:7.51.0-6.74.amzn1, libcurl-0:7.40.0-3.52.amzn1, libcurl-0:7.40.0-8.54.amzn1, libcurl-0:7.51.0-4.73.amzn1, libcurl-0:7.51.0-6.74.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000099

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-1000100

Severity
Low

Description
When doing a TFTP transfer and curl/libcurl is given a URL that contains a very long file name (longer than about 515 bytes), the file name is truncated to fit within the buffer boundaries, but the buffer size is still wrongly updated to use the untruncated length. This too large value is then used in the sendto() call, making curl attempt to send more data than what is actually put into the buffer. The endto() function will then read beyond the end of the heap based buffer. A malicious HTTP(S) server could redirect a vulnerable libcurl-using client to a crafted TFTP URL (if the client hasn't restricted which protocols it allows redirects to) and trick it to send private memory contents to a remote server over UDP. Limit curl's redirect protocols with --proto-redir and libcurl's with CURLOPT_REDIR_PROTOCOLS.

Recommendation
Use your Operating System's update feature to update package curl, curl-0:7.35.0-1ubuntu2.10, curl-0:7.35.0-1ubuntu2.5, curl-0:7.35.0-1ubuntu2.9, curl-0:7.40.0-3.52.amzn1, curl-0:7.40.0-8.54.amzn1, curl-0:7.51.0-4.73.amzn1, curl-0:7.51.0-6.74.amzn1, libcurl-0:7.40.0-3.52.amzn1, libcurl-0:7.40.0-8.54.amzn1, libcurl-0:7.51.0-4.73.amzn1, libcurl-0:7.51.0-6.74.amzn1, libcurl3, libcurl3-0:7.35.0-1ubuntu2.10, libcurl3-0:7.35.0-1ubuntu2.5, libcurl3-0:7.35.0-1ubuntu2.9, libcurl3-gnutls-0:7.35.0-1ubuntu2.10, libcurl3-gnutls-0:7.35.0-1ubuntu2.5, libcurl3-gnutls-0:7.35.0-1ubuntu2.9. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000100

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-1000101

Severity
Medium

Description
curl supports"globbing"of URLs, in which a user can pass a numerical range to have the tool iterate over those numbers to do a sequence oftransfers. In the globbing function that parses the numerical range, there was an omission that made curl read a byte beyond the end of theURL if given a carefully crafted, or just wrongly written, URL. The URL is stored in a heap based buffer, so it could then be made towrongly read something else instead of crashing. An example of a URL that triggers the flaw would be `http://ur%20[0-60000000000000000000`.

Recommendation
Use your Operating System's update feature to update package curl, curl-0:7.35.0-1ubuntu2.10, curl-0:7.35.0-1ubuntu2.5, curl-0:7.35.0-1ubuntu2.9, curl-0:7.40.0-3.52.amzn1, curl-0:7.40.0-8.54.amzn1, curl-0:7.51.0-4.73.amzn1, curl-0:7.51.0-6.74.amzn1, libcurl-0:7.40.0-3.52.amzn1, libcurl-0:7.40.0-8.54.amzn1, libcurl-0:7.51.0-4.73.amzn1, libcurl-0:7.51.0-6.74.amzn1, libcurl3, libcurl3-0:7.35.0-1ubuntu2.10, libcurl3-0:7.35.0-1ubuntu2.5, libcurl3-0:7.35.0-1ubuntu2.9, libcurl3-gnutls-0:7.35.0-1ubuntu2.10, libcurl3-gnutls-0:7.35.0-1ubuntu2.5, libcurl3-gnutls-0:7.35.0-1ubuntu2.9. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000101

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-1000111

Severity
High

Description
Linux kernel: heap out-of-bounds in AF_PACKET sockets. This new issue is analogous to previously disclosed CVE-2016-8655. In both cases, a socket option that changes socket state may race with safety checks in packet_set_ring. Previously with PACKET_VERSION. This time with PACKET_RESERVE. The solution is similar: lock the socket for the update. This issue may be exploitable, we did not investigate further. As this issue affects PF_PACKET sockets, it requires CAP_NET_RAW in the process namespace. But note that with user namespaces enabled, any process can create a namespace in which it has CAP_NET_RAW.

Recommendation
Use your Operating System's update feature to update package kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1, linux-image-3.13.0-63-generic, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000111

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-1000112

Severity
High

Description
Linux kernel: Exploitable memory corruption due to UFO to non-UFO path switch. When building a UFO packet with MSG_MORE __ip_append_data() calls

ip_ufo_append_data() to append. However in between two send() calls, the append path can be switched from UFO to non-UFO one, which leads to a memory corruption. In case UFO packet lengths exceeds MTU, copy = maxfraglen - skb->len becomes negative on the non-UFO path and the branch to allocate new skb is taken. This triggers fragmentation and computation of fraggap = skb_prev->len - maxfraglen. Fraggap can exceed MTU, causing copy = datalen - transhdrlen - fraggap to become negative. Subsequently skb_copy_and_csum_bits() writes out-of-bounds. A similar issue is present in IPv6 code. The bug was introduced in e89e9cf539a2 ("[IPv4/IPv6]: UFO Scatter-gather approach") on Oct 18 2005.

Recommendation
Use your Operating System's update feature to update package kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1, linux-image-3.13.0-63-generic, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000112

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-1000364

Severity
High

Description
An issue was discovered in the size of the stack guard page on Linux, specifically a 4k stack guard page is not sufficiently large and can be "jumped" over (the stack guard page is bypassed), this affects Linux Kernel versions 4.11.5 and earlier (the stackguard page was introduced in 2010).

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:2.6.32-431.11.2.el6, kernel-0:2.6.32-431.29.2.el6, kernel-0:2.6.32-431.el6, kernel-0:2.6.32-642.el6, kernel-0:2.6.32-696.el6, kernel-0:3.10.0-327.el7, kernel-0:3.10.0-514.16.1.el7, kernel-0:3.10.0-514.el7, kernel-0:3.14.48-33.39.amzn1,

kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1, kernel-devel-0:2.6.32-431.11.2.el6, kernel-firmware-0:2.6.32-431.11.2.el6, kernel-firmware-0:2.6.32-431.29.2.el6, kernel-firmware-0:2.6.32-642.el6, kernel-firmware-0:2.6.32-696.el6, kernel-headers-0:2.6.32-431.11.2.el6, kernel-headers-0:2.6.32-431.29.2.el6, kernel-headers-0:2.6.32-642.el6, kernel-tools-0:3.10.0-327.el7, kernel-tools-0:3.10.0-514.16.1.el7, kernel-tools-0:3.10.0-514.el7, kernel-tools-libs-0:3.10.0-327.el7, kernel-tools-libs-0:3.10.0-514.16.1.el7, kernel-tools-libs-0:3.10.0-514.el7, linux-image-3.13.0-55-generic, linux-image-3.13.0-55-generic-0:3.13.0-55.92, linux-image-3.13.0-63-generic, linux-image-3.13.0-63-generic-0:3.13.0-63.103, linux-image-3.19.0-21-generic, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual, linux-image-virtual-0:3.13.0.55.62-0, linux-image-virtual-0:3.13.0.63.71-0, perf-0:2.6.32-431.29.2.el6, perf-0:2.6.32-642.el6, python-perf, python-perf-0:3.10.0-327.el7, python-perf-0:3.10.0-514.16.1.el7, python-perf-0:3.10.0-514.el7. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000364

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-1000365

Severity
High

Description
The Linux Kernel imposes a size restriction on the arguments and environmental strings passed through RLIMIT_STACK/RLIM_INFINITY (1/4 of the size), but does not take the argument and environment pointers into account, which allows attackers to bypass this limitation. This affects Linux Kernel versions 4.11.5 and earlier. It appears that this feature was introduced in the Linux Kernel version 2.6.23.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1,

kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1, linux-image-3.13.0-63-generic, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000365

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-1000370

Severity
High

Description
The offset2lib patch as used in the Linux Kernel contains a vulnerability that allows a PIE binary to be execve()'ed with 1GB of arguments or environmental strings then the stack occupies the address 0x80000000 and the PIE binary is mapped above 0x40000000 nullifying the protection of the offset2lib patch. This affects Linux Kernel version 4.11.5 and earlier. This is a different issue than CVE-2017-1000371. This issue appears to be limited to i386 based systems.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000370

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-1000371

Severity
High

Description
The offset2lib patch as used by the Linux Kernel contains a vulnerability, if RLIMIT_STACK is set to RLIM_INFINITY and 1 Gigabyte of memory is allocated

(the maximum under the 1/4 restriction) then the stack will be grown down to 0x80000000, and as the PIE binary is mapped above 0x80000000 the minimum distance between the end of the PIE binary's read-write segment and the start of the stack becomes small enough that the stack guard page can be jumped over by an attacker. This affects Linux Kernel version 4.11.5. This is a different issue than CVE-2017-1000370 and CVE-2017-1000365. This issue appears to be limited to i386 based systems.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000371

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-1000377

Severity
Medium

Description
An issue was discovered in the size of the default stack guard page on PAX Linux (originally from GRSecurity but shipped by other Linux vendors), specifically the default stack guard page is not sufficiently large and can be "jumped" over (the stack guard page is bypassed), this affects PAX Linux Kernel versions as of June 19, 2017 (specific version information is not available at this time).

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-1000377

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-11473

Severity
High

Description
Buffer overflow in the mp_override_legacy_irq() function in arch/x86/kernel/acpi/boot.c in the Linux kernel through 4.12.2 allows local users to gain privileges via a crafted ACPI table.

Recommendation
Use your Operating System's update feature to update package kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-11473

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-12134

Severity
High

Description
The xen_biovec_phys_mergeable function in drivers/xen/biomerge.c in Xen might allow local OS guest users to corrupt block device data streams and consequently obtain sensitive memory information, cause a denial of service, or gain host OS privileges by leveraging incorrect block IO merge-ability calculation.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.44-39.55.amzn1, kernel-0:4.4.5-15.26.amzn1,

kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1, kernel-0:4.9.43-17.38.amzn1, kernel-headers-0:4.9.43-17.38.amzn1, kernel-tools-0:4.9.43-17.38.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12134

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-14497

Severity
High

Description
The tpacket_rcv function in net/packet/af_packet.c in the Linux kernel before 4.13 mishandles vnet headers, which might allow local users to cause a denial of service (buffer overflow, and disk and memory corruption) or possibly have unspecified other impact via crafted system calls.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.44-39.55.amzn1, kernel-0:4.4.5-15.26.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1, kernel-0:4.9.43-17.38.amzn1, kernel-0:4.9.43-17.39.amzn1, kernel-headers-0:4.9.43-17.38.amzn1, kernel-headers-0:4.9.43-17.39.amzn1, kernel-tools-0:4.9.43-17.38.amzn1, kernel-tools-0:4.9.43-17.39.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-14497

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-2616

Severity
Medium

Description
Sending SIGKILL to other processes with root privileges via su

Recommendation
Use your Operating System's update feature to update package coreutils-0:8.4-31.el6_5.2, coreutils-0:8.4-43.el6, coreutils-libs-0:8.4-31.el6_5.2, coreutils-libs-0:8.4-43.el6, libblkid-0:2.23.2-16.22.amzn1, libblkid-0:2.23.2-22.26.amzn1, libblkid-0:2.23.2-26.27.amzn1, libblkid-0:2.23.2-26.el7, libblkid-0:2.23.2-33.el7, libmount-0:2.23.2-16.22.amzn1, libmount-0:2.23.2-22.26.amzn1, libmount-0:2.23.2-26.27.amzn1, libmount-0:2.23.2-26.el7, libmount-0:2.23.2-33.el7, libuuid-0:2.23.2-16.22.amzn1, libuuid-0:2.23.2-22.26.amzn1, libuuid-0:2.23.2-26.27.amzn1, libuuid-0:2.23.2-26.el7, libuuid-0:2.23.2-33.el7, login, login-1:4.1.5.1-1ubuntu9, login-1:4.1.5.1-1ubuntu9.2, passwd, passwd-1:4.1.5.1-1ubuntu9, passwd-1:4.1.5.1-1ubuntu9.2, util-linux, util-linux-0:2.23.2-16.22.amzn1, util-linux-0:2.23.2-22.26.amzn1, util-linux-0:2.23.2-26.27.amzn1, util-linux-0:2.23.2-26.el7, util-linux-0:2.23.2-33.el7. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2616

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-2671

Severity
Medium

Description
The ping_unhash function in net/ipv4/ping.c in the Linux kernel through 4.10.8 is too late in obtaining a certain lock and consequently cannot ensure that disconnect function calls are safe, which allows local users to cause a denial of service (panic) by leveraging access to the protocol value of IPPROTO_ICMP in a socket system call.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.10.0-327.el7, kernel-0:3.10.0-514.el7, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-tools-0:3.10.0-327.el7, kernel-tools-0:3.10.0-514.el7, kernel-tools-libs-0:3.10.0-327.el7, kernel-tools-libs-0:3.10.0-514.el7, linux-image-3.13.0-63-generic, linux-image-3.13.0-63-generic-0:3.13.0-63.10

3, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual, python-perf-0:3.10.0-327.el7, python-perf-0:3.10.0-514.el7. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-2671

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-5967

Severity
Medium

Description
The time subsystem in the Linux kernel through 4.9.9, when CONFIG_TIMER_STATS is enabled, allows local users to discover real PID values (as distinguished from PID values inside a PID namespace) by reading the /proc/timer_list file, related to the print_timer function in kernel/time/timer_list.c and the __timer_stats_timer_set_start_info function in kernel/time/timer.c.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-5967

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-6451

Severity
Medium

Description
The mx4200_send function in the legacy MX4200 refclock in NTP before 4.2.8p10 and 4.3.x before 4.3.94 does not properly handle the return value of the snprintf function, which allows local users to execute arbitrary code via unspecified vectors, which trigger an out-of-bounds memory write.

Recommendation
Use your Operating System's update feature to update package ntp, ntp-0:4.2.6p5-36.29.amzn1, ntp-0:4.2.6p5-43.33.amzn1, ntpdate-0:4.2.6p5-36.29.amzn1, ntpdate-0:4.2.6p5-43.33.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6451

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-6458

Severity
High

Description
Multiple buffer overflows in the ctl_put* functions in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allow remote authenticated users to have unspecified impact via a long variable.

Recommendation
Use your Operating System's update feature to update package ntp, ntp-0:4.2.6p5-36.29.amzn1, ntp-0:4.2.6p5-43.33.amzn1, ntp-1:4.2.6.p5+dfsg-3ubuntu2.14.04.10, ntpdate-0:4.2.6p5-36.29.amzn1, ntpdate-0:4.2.6p5-43.33.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6458

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-6462

Severity
Medium

Description
Buffer overflow in the legacy Datum Programmable Time Server (DPTS) refclock driver in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows local users to have unspecified impact via a crafted /dev/datum device.

Recommendation

Use your Operating System's update feature to update package ntp, ntp-0:4.2.6p5-36.29.amzn1, ntp-0:4.2.6p5-43.33.amzn1, ntp-1:4.2.6.p5+dfsg-3ubuntu2.14.04.10, ntpdate-0:4.2.6p5-36.29.amzn1, ntpdate-0:4.2.6p5-43.33.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6462

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-6463

Severity
Medium

Description
NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote authenticated users to cause a denial of service (daemon crash) via an invalid setting in a :config directive, related to the unpeer option.

Recommendation
Use your Operating System's update feature to update package ntp, ntp-0:4.2.6p5-36.29.amzn1, ntp-0:4.2.6p5-43.33.amzn1, ntp-1:4.2.6.p5+dfsg-3ubuntu2.14.04.10, ntpdate-0:4.2.6p5-36.29.amzn1, ntpdate-0:4.2.6p5-43.33.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6463

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-6464

Severity
Medium

Description
NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote attackers to cause a denial of service (ntpd crash) via a malformed mode configuration directive.

Recommendation
Use your Operating System's update feature to update package ntp, ntp-0:4.2.6p5-36.29.amzn1, ntp-0:4.2.6p5-43.33.amzn1, ntp-1:4.2.6.p5+dfsg-3ubuntu2

.14.04.10, ntpdate-0:4.2.6p5-36.29.amzn1, ntpdate-0:4.2.6p5-43.33.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6464

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-7187

Severity
High

Description
The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel through 4.10.4 allows local users to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a large command size in an SG_NEXT_CMD_LEN ioctl call, leading to out-of-bounds write access in the sg_write function.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.10.0-327.el7, kernel-0:3.10.0-514.el7, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-tools-0:3.10.0-327.el7, kernel-tools-0:3.10.0-514.el7, kernel-tools-libs-0:3.10.0-327.el7, kernel-tools-libs-0:3.10.0-514.el7, linux-image-3.13.0-63-generic, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual, python-perf-0:3.10.0-327.el7, python-perf-0:3.10.0-514.el7. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7187

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-7308

Severity
High

Description
The packet_set_ring function in net/packet/af_packet.c in the Linux kernel through 4.10.6 does not properly validate certain block-size data, which allows local users to

cause a denial of service (integer signedness error and out-of-bounds write), or gain privileges (if the CAP_NET_RAW capability is held), via crafted system calls.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.10.0-327.el7, kernel-0:3.10.0-514.16.1.el7, kernel-0:3.10.0-514.el7, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-tools-0:3.10.0-327.el7, kernel-tools-0:3.10.0-514.16.1.el7, kernel-tools-0:3.10.0-514.el7, kernel-tools-libs-0:3.10.0-327.el7, kernel-tools-libs-0:3.10.0-514.16.1.el7, kernel-tools-libs-0:3.10.0-514.el7, linux-image-3.13.0-63-generic, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual, python-perf, python-perf-0:3.10.0-327.el7, python-perf-0:3.10.0-514.16.1.el7, python-perf-0:3.10.0-514.el7. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7308

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-7407

Severity
Medium

Description
The ourWriteOut function in tool_writeout.c in curl 7.53.1 might allow physically proximate attackers to obtain sensitive information from process memory in opportunistic circumstances by reading a workstation screen during use of a --write-out argument ending in a '%' character, which leads to a heap-based buffer over-read.

Recommendation
Use your Operating System's update feature to update package curl, curl-0:7.35.0-1ubuntu2.10, curl-0:7.35.0-1ubuntu2.5, curl-0:7.35.0-1ubuntu2.9, curl-0:7.40.0-3.52.amzn1, curl-0:7.40.0-8.54.amzn1, curl-0:7.51.0-4.73.amzn1, libcurl-0:7.40.0-3.52.amzn1, libcurl-0:7.40.0-8.54.amzn1, libcurl-0:7.51.0-4.73.amzn1, libcurl3, libcurl3-0:7.35.0-1ubuntu2.10, libcurl3-0:7.35.0-1ubuntu2.5, libcurl3-0:7.35.0-1ubuntu2.9, libcurl3-gnutls-0:7.35.0-1ubuntu2.10, libcurl3-gnutls-0:7.35.0-1ubuntu2.5, libcurl3-gnutls-0:7.35.0-1ubuntu2.9. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7407

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-7488

Severity
Medium

Description
Authconfig version 6.2.8 is vulnerable to an Information exposure while using SSSD to authenticate against remote server resulting in the leak of information about existing usernames.

Recommendation
Use your Operating System's update feature to update package authconfig-0:6.1 .12-23.25.amzn1, authconfig-0:6.2.8-10.28.amzn1, authconfig-0:6.2.8-10.el7, authconfig-0:6.2.8-14.el7, authconfig-0:6.2.8-9.27.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7488

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-7533

Severity
High

Description
Race condition in the fsnotify implementation in the Linux kernel through 4.12.4 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that leverages simultaneous execution of the inotify_handle_event and vfs_rename functions.

Recommendation
Use your Operating System's update feature to update package kernel-0:3.10.0-327.el7, kernel-0:3.10.0-514.el7, kernel-0:3.10.0-693.el7, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1, kernel-tools-0:3.10.0-327.el7, kernel-

tools-0:3.10.0-514.el7, kernel-tools-0:3.10.0-693.el7, kernel-tools-libs-0:3.10.0-3
27.el7, kernel-tools-libs-0:3.10.0-514.el7, kernel-tools-libs-0:3.10.0-693.el7, linux-
image-3.13.0-63-generic, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-
lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual, python-perf-0:3.10.0-327.el7,
python-perf-0:3.10.0-514.el7, python-perf-0:3.10.0-693.el7. For more information see
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7533

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-7542

Severity
Medium

Description
The ip6_find_1stfragopt function in net/ipv6/output_core.c in the Linux kernel through 4.12.3 allows local users to cause a denial of service (integer overflow and infinite loop) by leveraging the ability to open a raw socket.

Recommendation
Use your Operating System's update feature to update package
kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1,
kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1,
kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1,
kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1. For more information see
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7542

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-7558

Severity
Low

Description
sctp: out-of-bounds read in inet_diag_msg_sctp{,l}addr_fill() and sctp_get_sctp_info()

Recommendation

Use your Operating System's update feature to update package kernel, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.44-39.55.amzn1, kernel-0:4.4.5-15.26.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1, kernel-0:4.9.43-17.38.amzn1, kernel-0:4.9.43-17.39.amzn1, kernel-headers-0:4.9.43-17.38.amzn1, kernel-headers-0:4.9.43-17.39.amzn1, kernel-tools-0:4.9.43-17.38.amzn1, kernel-tools-0:4.9.43-17.39.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7558

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-7616

Severity
Medium

Description
Incorrect error handling in the set_mempolicy and mbind compat syscalls in mm/mempolicy.c in the Linux kernel through 4.10.9 allows local users to obtain sensitive information from uninitialized stack data by triggering failure of a certain bitmap operation.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.10.0-327.el7, kernel-0:3.10.0-514.el7, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-tools-0:3.10.0-327.el7, kernel-tools-0:3.10.0-514.el7, kernel-tools-libs-0:3.10.0-327.el7, kernel-tools-libs-0:3.10.0-514.el7, linux-image-3.13.0-63-generic, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual, python-perf-0:3.10.0-327.el7, python-perf-0:3.10.0-514.el7. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7616

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-7618

Severity
High

Description
crypto/ahash.c in the Linux kernel through 4.10.9 allows attackers to cause a denial of service (API operation calling its own callback, and infinite recursion) by triggering EBUSY on a full queue.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, linux-image-3.13.0-63-generic, linux-image-3.13.0-63-generic-0:3.13.0-63.103, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-7618

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-8831

Severity
High

Description
The saa7164_bus_get function in drivers/media/pci/saa7164/saa7164-bus.c in the Linux kernel through 4.11.5 allows local users to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact by changing a certain sequence-number value, aka a "double fetch" vulnerability.

Recommendation
Use your Operating System's update feature to update package kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1, linux-image-3.13.0-63-generic, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-lowlatency-0:4.4.0-

47.68~14.04.1, linux-image-virtual. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8831

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-8890

Severity
High

Description
The inet_csk_clone_lock function in net/ipv4/inet_connection_sock.c in the Linux kernel through 4.10.15 allows attackers to cause a denial of service (double free) or possibly have unspecified other impact by leveraging use of the accept system call.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.10.0-327.el7, kernel-0:3.10.0-514.el7, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1, kernel-tools-0:3.10.0-327.el7, kernel-tools-0:3.10.0-514.el7, kernel-tools-libs-0:3.10.0-327.el7, kernel-tools-libs-0:3.10.0-514.el7, linux-image-3.13.0-55-generic, linux-image-3.13.0-55-generic-0:3.13.0-55.92, linux-image-3.13.0-63-generic, linux-image-3.13.0-63-generic-0:3.13.0-63.103, linux-image-3.19.0-21-generic, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual, linux-image-virtual-0:3.13.0.55.62-0, linux-image-virtual-0:3.13.0.63.71-0, python-perf-0:3.10.0-327.el7, python-perf-0:3.10.0-514.el7. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8890

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-9059

Severity
Medium

Description
The NFSv4 implementation in the Linux kernel through 4.11.1 allows local users to cause a denial of service (resource consumption) by leveraging improper channel callback shutdown when unmounting an NFSv4 filesystem, aka a "module reference and kernel daemon" leak.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9059

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-9074

Severity
High

Description
The IPv6 fragmentation implementation in the Linux kernel through 4.11.1 does not consider that the nexthdr field may be associated with an invalid option, which allows local users to cause a denial of service (out-of-bounds read and BUG) or possibly have unspecified other impact via crafted socket and send system calls.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.10.0-327.el7, kernel-0:3.10.0-514.el7, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1, kernel-tools-0:3.10.0-327.el7, kernel-tools-0:3.10.0-514.el7, kernel-tools-libs-0:3.10.0-327.el7, kernel-tools-libs-0:3.10.0-514.el7, linux-image-3.13.0-55-generic, linux-image-3.13.0-55-generic-0:3.13.0-55.92, linux-image-3.13.0-63-generic, linux-image-3.13.0-63-generic-0:3.13.0-63.103, linux-image-3.19.0-21-generic, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-

lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual, linux-image-virtual-0:3.13.0.55.62-0, linux-image-virtual-0:3.13.0.63.71-0, python-perf-0:3.10.0-327.el7, python-perf-0:3.10.0-514.el7. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9074

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-9075

Severity
High

Description
The sctp_v6_create_accept_sk function in net/sctp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.10.0-327.el7, kernel-0:3.10.0-514.el7, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1, kernel-tools-0:3.10.0-327.el7, kernel-tools-0:3.10.0-514.el7, kernel-tools-libs-0:3.10.0-327.el7, kernel-tools-libs-0:3.10.0-514.el7, linux-image-3.13.0-55-generic, linux-image-3.13.0-55-generic-0:3.13.0-55.92, linux-image-3.13.0-63-generic, linux-image-3.13.0-63-generic-0:3.13.0-63.103, linux-image-3.19.0-21-generic, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual, linux-image-virtual-0:3.13.0.55.62-0, linux-image-virtual-0:3.13.0.63.71-0, python-perf-0:3.10.0-327.el7, python-perf-0:3.10.0-514.el7. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9075

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-9076

Severity
High

Description
The dccp_v6_request_recv_sock function in net/dccp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.10.0-327.el7, kernel-0:3.10.0-514.el7, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1, kernel-tools-0:3.10.0-327.el7, kernel-tools-0:3.10.0-514.el7, kernel-tools-libs-0:3.10.0-327.el7, kernel-tools-libs-0:3.10.0-514.el7, linux-image-3.13.0-55-generic, linux-image-3.13.0-55-generic-0:3.13.0-55.92, linux-image-3.13.0-63-generic, linux-image-3.13.0-63-generic-0:3.13.0-63.103, linux-image-3.19.0-21-generic, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual, linux-image-virtual-0:3.13.0.55.62-0, linux-image-virtual-0:3.13.0.63.71-0, python-perf-0:3.10.0-327.el7, python-perf-0:3.10.0-514.el7. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9076

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-9077

Severity
High

Description
The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.10.0-327.el7, kernel-0:3.10.0-514.el7, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1, kernel-tools-0:3.10.0-327.el7, kernel-tools-0:3.10.0-514.el7, kernel-tools-libs-0:3.10.0-327.el7, kernel-tools-libs-0:3.10.0-514.el7, linux-image-3.13.0-55-generic, linux-image-3.13.0-55-generic-0:3.13.0-55.92, linux-image-3.13.0-63-generic, linux-image-3.13.0-63-generic-0:3.13.0-63.103, linux-image-3.19.0-21-generic, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual, linux-image-virtual-0:3.13.0.55.62-0, linux-image-virtual-0:3.13.0.63.71-0, python-perf-0:3.10.0-327.el7, python-perf-0:3.10.0-514.el7. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9077

Failed Instances
i-035c60a4c31f51e7b

CVE-2017-9242

Severity
Medium

Description
The __ip6_append_data function in net/ipv6/ip6_output.c in the Linux kernel through 4.11.3 is too late in checking whether an overwrite of an skb data structure may occur, which allows local users to cause a denial of service (system crash) via crafted system calls.

Recommendation
Use your Operating System's update feature to update package kernel, kernel-0:3.10.0-327.el7, kernel-0:3.10.0-514.el7, kernel-0:3.14.48-33.39.amzn1, kernel-0:4.1.17-22.30.amzn1, kernel-0:4.4.23-31.54.amzn1, kernel-0:4.4.41-36.55.amzn1, kernel-0:4.4.51-40.58.amzn1, kernel-0:4.4.8-20.46.amzn1, kernel-0:4.9.17-6.29.amzn1, kernel-0:4.9.20-11.31.amzn1, kernel-0:4.9.27-14.31.amzn1, kernel-tools-0:3.10.0-327.el7, kernel-tools-0:3.10.0-514.el7, kernel-tools-libs-0:3.10.0-327.el7, kernel-tools-libs-0:3.10.0-514.el7, linux-image-3.13.0-55-generic, linux-image-3.13.0-55-generic-0:3.13.0-55.92,

linux-image-3.13.0-63-generic, linux-image-3.13.0-63-generic-0:3.13.0-63.103, linux-image-3.19.0-21-generic, linux-image-4.4.0-47-lowlatency, linux-image-4.4.0-47-lowlatency-0:4.4.0-47.68~14.04.1, linux-image-virtual, linux-image-virtual-0:3.13.0.55.62-0, linux-image-virtual-0:3.13.0.63.71-0, python-perf-0:3.10.0-327.el7, python-perf-0:3.10.0-514.el7. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9242

Failed Instances
i-035c60a4c31f51e7b

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-2009-2408	Mozilla Network Security Services (NSS) before 3.12.3, Firefox before 3.0.13, Thunderbird before 2.0.0.23, and SeaMonkey before 1.1.18 do not properly handle a '\0' character in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority. NOTE: this was originally reported for Firefox before 3.5.
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-2009-3293	Unspecified vulnerability in the imagecolortransparent function in PHP before 5.2.11 has unknown impact and attack vectors related to an incorrect "sanity check for the color index."
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-2009-3546	The _gdGetColors function in gd_gd.c in PHP 5.2.11 and 5.3.x before 5.3.1, and the GD Graphics Library 2.x, does not properly verify a certain colorsTotal structure member, which might allow remote attackers to conduct buffer overflow or buffer over-read attacks via a crafted GD file, a different vulnerability than CVE-2009-3293. NOTE: some of these details are obtained from third party information.
CVE-2009-3743	Off-by-one error in the Ins_MINDEX function in the TrueType bytecode interpreter in Ghostscript before 8.71 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via a malformed TrueType font in a document that trigger an integer overflow and a heap-based buffer overflow.
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-2009-4307	The ext4_fill_flex_info function in fs/ext4/super.c in the Linux kernel before 2.6.32-git6 allows user-assisted remote attackers to cause a denial of service (divide-by-zero error and panic) via a malformed ext4 filesystem containing a super block with a large FLEX_BG group size (aka s_log_groups_per_flex value).
CVE-2009-5029	Integer overflow in the __tzfile_read function in glibc before 2.15 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted timezone (TZ) file, as demonstrated using vsftpd.
CVE-2009-5030	The tcd_free_encode function in tcd.c in OpenJPEG 1.3 through 1.5 allows remote attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code via crafted tile information in a Gray16 TIFF image, which causes insufficient memory to be allocated and leads to an "invalid free."
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-2010-2055	Ghostscript 8.71 and earlier reads initialization files from the current working directory, which allows local users to execute arbitrary PostScript commands via a Trojan horse file, related to improper support for the -P- option to the gs program, as demonstrated using gs_init.ps, a different vulnerability than CVE-2010-4820.
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-2010-2596	The OJPEGPostDecode function in tif_ojpeg.c in LibTIFF 3.9.0 and 3.9.2, as used in tiff2ps, allows remote attackers to cause a denial of service (assertion

	failure and application exit) via a crafted TIFF image, related to "downsampled OJPEG input."
CVE-2010-2642	Heap-based buffer overflow in the AFM font parser in the dvi-backend component in Evince 2.32 and earlier, teTeX 3.0, t1lib 5.1.2, and possibly other products allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted font in conjunction with a DVI file that is processed by the thumbnailer.
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-2010-3294	Cross-site scripting (XSS) vulnerability in apc.php in the Alternative PHP Cache (APC) extension before 3.1.4 for PHP allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
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-2010-4054	The gs_type2_interpret function in Ghostscript allows remote attackers to cause a denial of service (incorrect pointer dereference and application crash) via crafted font data in a compressed data stream, aka bug 691043.
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-2010-4167	Untrusted search path vulnerability in configure.c in ImageMagick before 6.6.5-5, when MAGICKCORE_INSTALLED_SUPPORT is defined, allows local users to gain privileges via a Trojan horse configuration file in the current working directory.
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-2010-4818	The GLX extension in X.Org xserver 1.7.7 allows remote authenticated users to cause a denial of service (server crash) and possibly execute arbitrary code via (1) a crafted request that triggers a client swap in glx/glxcmdsswap.c; or (2) a crafted length or (3) a negative value in the screen field in a request to glx/glxcmds.c.
CVE-2010-4819	The ProcRenderAddGlyphs function in the Render extension (render/render.c) in X.Org xserver 1.7.7 and earlier allows local users to read arbitrary memory and possibly cause a denial of service (server crash) via unspecified vectors related to an "input sanitization flaw."
CVE-2010-4820	Untrusted search path vulnerability in Ghostscript 8.62 allows local users to execute arbitrary PostScript code via a Trojan horse Postscript library file in Encoding/ under the current working directory, a different vulnerability than CVE-2010-2055.
CVE-2010-5298	Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.
CVE-2010-5325	Heap-based buffer overflow in the unhtmlify function in foomatic-rip in foomatic-filters before 4.0.6 allows remote attackers to cause a denial of service (memory corruption and crash) or possibly execute arbitrary code via a long job title.
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-2011-0633	The Net::HTTPS module in libwww-perl (LWP) before 6.00, as used in WWW::Mechanize, LWP::UserAgent, and other products, when running in environments that do not set the If-SSL-Cert-Subject header, does not enable full validation of SSL certificates by default, which allows remote attackers to spoof servers via man-in-the-middle (MITM) attacks involving hostnames that are not properly validated. NOTE: it could be argued that this is a design limitation of the Net::HTTPS API, and separate implementations should be independently assigned CVE identifiers for not working around this limitation. However, because this API was modified within LWP, a single CVE identifier has been assigned.
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-2011-0764	t1lib 5.1.2 and earlier, as used in Xpdf before 3.02pl6, teTeX, and other products, uses an invalid pointer in conjunction with a dereference operation, which allows remote attackers to execute arbitrary code via a crafted Type 1 font in a PDF document, as demonstrated by testz.2184122398.pdf.
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-2011-1005	The safe-level feature in Ruby 1.8.6 through 1.8.6-420, 1.8.7 through 1.8.7-330, and 1.8.8dev allows context-dependent attackers to modify strings via the Exception#to_s method, as demonstrated by changing an intended pathname.
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-2011-1083	The epoll implementation in the Linux kernel 2.6.37.2 and earlier does not properly traverse a tree of epoll file descriptors, which allows local users to cause a denial of service (CPU consumption) via a crafted application that makes epoll_create and epoll_ctl system calls.

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-2011-1143	epan/dissectors/packet-ntlmssp.c in the NTLMSSP dissector in Wireshark before 1.4.4 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted .pcap file.

CVE-2011-1148	Use-after-free vulnerability in the substr_replace function in PHP 5.3.6 and earlier allows context-dependent attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact by using the same variable for multiple arguments.
CVE-2011-1162	The tpm_read function in the Linux kernel 2.6 does not properly clear memory, which might allow local users to read the results of the previous TPM command.
CVE-2011-1184	The HTTP Digest Access Authentication implementation in Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.12 does not have the expected countermeasures against replay attacks, which makes it easier for remote attackers to bypass intended access restrictions by sniffing the network for valid requests, related to lack of checking of nonce (aka server nonce) and nc (aka nonce-count or client nonce count) values.
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-2011-1527	The kdb_ldap plugin in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.9 through 1.9.1, when the LDAP back end is used, allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a kinit operation with incorrect string case for the realm, related to the is_principal_in_realm, krb5_set_error_message, krb5_ldap_get_principal, and process_as_req functions.
CVE-2011-1530	The process_tgs_req function in do_tgs_req.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.9 through 1.9.2 allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted TGS request that triggers an error other than the KRB5_KDB_NOENTRY error.
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-2011-1552	t1lib 5.1.2 and earlier, as used in Xpdf before 3.02pl6, teTeX, and other products, reads from invalid memory locations, which allows remote attackers to cause a denial of service (application crash) via a crafted Type 1 font in a PDF document, a different vulnerability than CVE-2011-0764.
CVE-2011-1553	Use-after-free vulnerability in t1lib 5.1.2 and earlier, as used in Xpdf before 3.02pl6, teTeX, and other products, allows remote attackers to cause a denial of service (application crash) via a PDF document containing a crafted Type 1 font that triggers an invalid memory write, a different vulnerability than CVE-2011-0764.
CVE-2011-1554	Off-by-one error in t1lib 5.1.2 and earlier, as used in Xpdf before 3.02pl6, teTeX, and other products, allows remote attackers to cause a denial of service (application crash) via a PDF document containing a crafted Type 1 font that triggers an invalid memory read, integer overflow, and invalid pointer dereference, a different vulnerability than CVE-2011-0764.
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-2011-1577	Heap-based buffer overflow in the is_gpt_valid function in fs/partitions/efi.c in the Linux kernel 2.6.38 and earlier allows physically proximate attackers to cause a denial of service (OOPS) or possibly have unspecified other impact via a crafted size of the EFI GUID partition-table header on removable media.
CVE-2011-1590	The X.509if dissector in Wireshark 1.2.x before 1.2.16 and 1.4.x before 1.4.5 does not properly initialize certain global variables, which allows remote attackers to cause a denial of service (application crash) via a crafted .pcap file.
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-2011-1833	Race condition in the ecryptfs_mount function in fs/ecryptfs/main.c in the eCryptfs subsystem in the Linux kernel before 3.1 allows local users to bypass intended file permissions via a mount.ecryptfs_private mount with a mismatched uid.
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-2011-1938	Stack-based buffer overflow in the socket_connect function in ext/sockets/sockets.c in PHP 5.3.3 through 5.3.6 might allow context-dependent attackers to execute arbitrary code via a long pathname for a UNIX socket.
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-2011-2179	Multiple cross-site scripting (XSS) vulnerabilities in config.c in config.cgi in (1) Nagios 3.2.3 and (2) Icinga before 1.4.1 allow remote attackers to inject arbitrary web script or HTML via the expand parameter, as demonstrated by an (a) command action or a (b) hosts action.
CVE-2011-2202	The rfc1867_post_handler function in main/rfc1867.c in PHP before 5.3.7 does not properly restrict filenames in multipart/form-data POST requests, which allows remote attackers to conduct absolute path traversal attacks, and possibly create or overwrite arbitrary files, via a crafted upload request, related to a "file path injection vulnerability."
CVE-2011-2204	Apache Tomcat 5.5.x before 5.5.34, 6.x before 6.0.33, and 7.x before 7.0.17, when the MemoryUserDatabase is used, creates log entries containing passwords upon encountering errors in JMX user creation, which allows local users to obtain sensitive information by reading a log file.
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-2011-2262	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote attackers to affect availability via unknown vectors.

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-2011-2483	crypt_blowfish before 1.1, as used in PHP before 5.3.7 on certain platforms, PostgreSQL before 8.4.9, and other products, does not properly handle 8-bit characters, which makes it easier for context-dependent attackers to determine a cleartext password by leveraging knowledge of a password hash.
CVE-2011-2494	kernel/taskstats.c in the Linux kernel before 3.1 allows local users to obtain sensitive I/O statistics by sending taskstats commands to a netlink socket, as demonstrated by discovering the length of another user's password.
CVE-2011-2699	The IPv6 implementation in the Linux kernel before 3.1 does not generate Fragment Identification values separately for each destination, which makes it easier for remote attackers to cause a denial of service (disrupted networking) by predicting these values and sending crafted packets.
CVE-2011-2716	The DHCP client (udhcpc) in BusyBox before 1.20.0 allows remote DHCP servers to execute arbitrary commands via shell metacharacters in the (1) HOST_NAME, (2) DOMAIN_NAME, (3) NIS_DOMAIN, and (4) TFTP_SERVER_NAME host name options.
CVE-2011-2723	The skb_gro_header_slow function in include/linux/netdevice.h in the Linux kernel before 2.6.39.4, when Generic Receive Offload (GRO) is enabled, resets certain fields in incorrect situations, which allows remote attackers to cause a denial of service (system crash) via crafted network traffic.
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-2011-2766	The FCGI (aka Fast CGI) module 0.70 through 0.73 for Perl, as used by CGI::Fast, uses environment variable values from one request during processing of a later request, which allows remote attackers to bypass authentication via crafted HTTP headers.
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-2011-2905	Untrusted search path vulnerability in the perf_config function in tools/perf/util/config.c in perf, as distributed in the Linux kernel before 3.1, allows local users to overwrite arbitrary files via a crafted config file in the current working directory.
CVE-2011-2918	The Performance Events subsystem in the Linux kernel before 3.1 does not properly handle event overflows associated with PERF_COUNT_SW_CPU_CLOCK events, which allows local users to cause a denial of service (system hang) via a crafted application.
CVE-2011-2939	Off-by-one error in the decode_xs function in Unicode/Unicode.xs in the Encode module before 2.44, as used in Perl before 5.15.6, might allow context-dependent attackers to cause a denial of service (memory corruption) via a crafted Unicode string, which triggers a heap-based buffer overflow.
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-2011-3048	The png_set_text_2 function in pngset.c in libpng 1.0.x before 1.0.59, 1.2.x before 1.2.49, 1.4.x before 1.4.11, and 1.5.x before 1.5.10 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted text chunk in a PNG image file, which triggers a memory allocation failure that is not properly handled, leading to a heap-based buffer overflow.
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-2011-3148	Stack-based buffer overflow in the _assemble_line function in modules/pam_env/pam_env.c in Linux-PAM (aka pam) before 1.1.5 allows local users to cause a denial of service (crash) and possibly execute arbitrary code via a long string of white spaces at the beginning of the ~/.pam_environment file.
CVE-2011-3149	The _expand_arg function in the pam_env module (modules/pam_env/pam_env.c) in Linux-PAM (aka pam) before 1.1.5 does not properly handle when environment variable expansion can overflow, which allows local users to cause a denial of service (CPU consumption).
CVE-2011-3182	PHP before 5.3.7 does not properly check the return values of the malloc, calloc, and realloc library functions, which allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) or trigger a buffer overflow by leveraging the ability to provide an arbitrary value for a function argument, related to (1) ext/curl/interface.c, (2) ext/date/lib/parse_date.c, (3) ext/date/lib/parse_iso_intervals.c, (4) ext/date/lib/parse_tz.c, (5) ext/date/lib/timelib.c, (6) ext/pdo_odbc/pdo_odbc.c, (7) ext/reflection/php_reflection.c, (8) ext/soap/php_sdl.c, (9) ext/xmlrpc/libxmlrpc/base64.c, (10) TSRM/tsrm_win32.c, and (11) the strtotime function.
CVE-2011-3188	The (1) IPv4 and (2) IPv6 implementations in the Linux kernel before 3.1 use a modified MD4 algorithm to generate sequence numbers and Fragment

	Identification values, which makes it easier for remote attackers to cause a denial of service (disrupted networking) or hijack network sessions by predicting these values and sending crafted packets.
CVE-2011-3190	Certain AJP protocol connector implementations in Apache Tomcat 7.0.0 through 7.0.20, 6.0.0 through 6.0.33, 5.5.0 through 5.5.33, and possibly other versions allow remote attackers to spoof AJP requests, bypass authentication, and obtain sensitive information by causing the connector to interpret a request body as a new request.
CVE-2011-3191	Integer signedness error in the CIFSFindNext function in fs/cifs/cifssmb.c in the Linux kernel before 3.1 allows remote CIFS servers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a large length value in a response to a read request for a directory.
CVE-2011-3192	The byterange filter in the Apache HTTP Server 1.3.x, 2.0.x through 2.0.64, and 2.2.x through 2.2.19 allows remote attackers to cause a denial of service (memory and CPU consumption) via a Range header that expresses multiple overlapping ranges, as exploited in the wild in August 2011, a different vulnerability than CVE-2007-0086.
CVE-2011-3207	crypto/x509/x509_vfy.c in OpenSSL 1.0.x before 1.0.0e does not initialize certain structure members, which makes it easier for remote attackers to bypass CRL validation by using a nextUpdate value corresponding to a time in the past.
CVE-2011-3208	Stack-based buffer overflow in the split_wildmats function in nntpd.c in nntpd in Cyrus IMAP Server before 2.3.17 and 2.4.x before 2.4.11 allows remote attackers to execute arbitrary code via a crafted NNTP command.
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-2011-3256	FreeType 2 before 2.4.7, as used in CoreGraphics in Apple iOS before 5, Mandriva Enterprise Server 5, and possibly other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted font, a different vulnerability than CVE-2011-0226.
CVE-2011-3348	The mod_proxy_ajp module in the Apache HTTP Server before 2.2.21, when used with mod_proxy_balancer in certain configurations, allows remote attackers to cause a denial of service (temporary "error state" in the backend server) via a malformed HTTP request.

CVE-2011-3353	Buffer overflow in the fuse_notify_inval_entry function in fs/fuse/dev.c in the Linux kernel before 3.1 allows local users to cause a denial of service (BUG_ON and system crash) by leveraging the ability to mount a FUSE filesystem.
CVE-2011-3359	The dma_rx function in drivers/net/wireless/b43/dma.c in the Linux kernel before 2.6.39 does not properly allocate receive buffers, which allows remote attackers to cause a denial of service (system crash) via a crafted frame.
CVE-2011-3363	The setup_cifs_sb function in fs/cifs/connect.c in the Linux kernel before 2.6.39 does not properly handle DFS referrals, which allows remote CIFS servers to cause a denial of service (system crash) by placing a referral at the root of a share.
CVE-2011-3368	The mod_proxy module in the Apache HTTP Server 1.3.x through 1.3.42, 2.0.x through 2.0.64, and 2.2.x through 2.2.21 does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers via a malformed URI containing an initial @ (at sign) character.
CVE-2011-3372	imap/nntpd.c in the NNTP server (nntpd) for Cyrus IMAPd 2.4.x before 2.4.12 allows remote attackers to bypass authentication by sending an AUTHINFO USER command without sending an additional AUTHINFO PASS command.
CVE-2011-3378	RPM 4.4.x through 4.9.x, probably before 4.9.1.2, allows remote attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code via an rpm package with crafted headers and offsets that are not properly handled when a package is queried or installed, related to (1) the regionSwab function, (2) the headerLoad function, and (3) multiple functions in rpmio/rpmpgp.c.
CVE-2011-3379	The is_a function in PHP 5.3.7 and 5.3.8 triggers a call to the __autoload function, which makes it easier for remote attackers to execute arbitrary code by providing a crafted URL and leveraging potentially unsafe behavior in certain PEAR packages and custom autoloaders.
CVE-2011-3380	Openswan 2.6.29 through 2.6.35 allows remote attackers to cause a denial of service (NULL pointer dereference and pluto IKE daemon crash) via an ISAKMP message with an invalid KEY_LENGTH attribute, which is not properly handled by the error handling function.
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-2011-3439	FreeType in CoreGraphics in Apple iOS before 5.0.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted font in a document.
CVE-2011-3481	The index_get_ids function in index.c in imapd in Cyrus IMAP Server before 2.4.11, when server-side threading is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted References header in an e-mail message.
CVE-2011-3521	Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE, 7, 6 Update 27 and earlier, and 5.0 Update 31 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect confidentiality, integrity, and availability via unknown vectors related to Deserialization.
CVE-2011-3544	Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7 and 6 Update 27 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect confidentiality, integrity, and availability via unknown vectors related to Scripting.
CVE-2011-3547	Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7, 6 Update 27 and earlier, 5.0 Update 31 and earlier, and 1.4.2_33 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect confidentiality via unknown vectors related to Networking.

CVE-2011-3548	Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7, 6 Update 27 and earlier, 5.0 Update 31 and earlier, and 1.4.2_33 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect confidentiality, integrity, and availability, related to AWT.
CVE-2011-3551	Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7, 6 Update 27 and earlier, and JRockit R28.1.4 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.
CVE-2011-3552	Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7, 6 Update 27 and earlier, 5.0 Update 31 and earlier, and 1.4.2_33 and earlier allows remote attackers to affect integrity via unknown vectors related to Networking.
CVE-2011-3553	Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7, 6 Update 27 and earlier, and JRockit R28.1.4 and earlier allows remote authenticated users to affect confidentiality, related to JAXWS.
CVE-2011-3554	Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7, 6 Update 27 and earlier, 5.0 Update 31 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect confidentiality, integrity, and availability via unknown vectors.
CVE-2011-3556	Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7, 6 Update 27 and earlier, 5.0 Update 31 and earlier, 1.4.2_33 and earlier, and JRockit R28.1.4 and earlier allows remote attackers to affect confidentiality, integrity, and availability, related to RMI, a different vulnerability than CVE-2011-3557.
CVE-2011-3557	Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7, 6 Update 27 and earlier, 5.0 Update 31 and earlier, 1.4.2_33 and earlier, and JRockit R28.1.4 and earlier allows remote attackers to affect confidentiality, integrity, and availability, related to RMI, a different vulnerability than CVE-2011-3556.
CVE-2011-3558	Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7, 6 Update 27 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets

	to affect confidentiality via unknown vectors related to HotSpot.
CVE-2011-3560	Unspecified vulnerability in the Java Runtime Environment component in Oracle Java SE JDK and JRE 7, 6 Update 27 and earlier, 5.0 Update 31 and earlier, and 1.4.2_33 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect confidentiality and integrity, related to JSSE.
CVE-2011-3563	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, 5.0 Update 33 and earlier, and 1.4.2_35 and earlier allows remote attackers to affect confidentiality and availability via unknown vectors related to Sound.
CVE-2011-3571	Unspecified vulnerability in the Virtual Desktop Infrastructure (VDI) component in Oracle Virtualization 3.2 allows remote authenticated users to affect confidentiality and integrity via unknown vectors related to Session. NOTE: this CVE identifier was accidentally used for a Concurrency issue in Java Runtime Environment, but that issue has been reassigned to CVE-2012-0507.
CVE-2011-3593	A certain Red Hat patch to the vlan_hwaccel_do_receive function in net/8021q/vlan_core.c in the Linux kernel 2.6.32 on Red Hat Enterprise Linux (RHEL) 6 allows remote attackers to cause a denial of service (system crash) via priority-tagged VLAN frames.
CVE-2011-3597	Eval injection vulnerability in the Digest module before 1.17 for Perl allows context-dependent attackers to execute arbitrary commands via the new constructor.
CVE-2011-3607	Integer overflow in the ap_pregsub function in server/util.c in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x through 2.2.21, when the mod_setenvif module is enabled, allows local users to gain privileges via a .htaccess file with a crafted SetEnvIf directive, in conjunction with a crafted HTTP request header, leading to a heap-based buffer overflow.
CVE-2011-3639	The mod_proxy module in the Apache HTTP Server 2.0.x through 2.0.64 and 2.2.x before 2.2.18, when the Revision 1179239 patch is in place, does not properly interact with use of (1) RewriteRule and (2) ProxyPassMatch pattern matches for configuration of a reverse proxy, which allows remote attackers to send requests to intranet servers by using the HTTP/0.9 protocol with a malformed URI containing an initial @ (at sign) character. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-3368.

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-2011-3869	Puppet 2.7.x before 2.7.5, 2.6.x before 2.6.11, and 0.25.x allows local users to overwrite arbitrary files via a symlink attack on the .k5login file.
CVE-2011-3870	Puppet 2.7.x before 2.7.5, 2.6.x before 2.6.11, and 0.25.x allows local users to modify the permissions of arbitrary files via a symlink attack on the SSH authorized_keys file.
CVE-2011-3871	Puppet 2.7.x before 2.7.5, 2.6.x before 2.6.11, and 0.25.x, when running in --edit mode, uses a predictable file name, which allows local users to run arbitrary Puppet code or trick a user into editing arbitrary files.
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-2011-4028	The LockServer function in os/utils.c in X.Org xserver before 1.11.2 allows local users to determine the existence of arbitrary files via a symlink attack on a temporary lock file, which is handled differently if the file exists.
CVE-2011-4029	The LockServer function in os/utils.c in X.Org xserver before 1.11.2 allows local users to change the permissions of arbitrary files to 444, read those files, and possibly cause a denial of service (removed execution permission) via a symlink attack on a temporary lock file.
CVE-2011-4073	Use-after-free vulnerability in the cryptographic helper handler functionality in Openswan 2.3.0 through 2.6.36 allows remote authenticated users to cause a denial of service (pluto IKE daemon crash) via vectors related to the (1) quick_outI1_continue and (2) quick_outI1 functions.
CVE-2011-4077	Buffer overflow in the xfs_readlink function in fs/xfs/xfs_vnodeops.c in XFS in the Linux kernel 2.6, when CONFIG_XFS_DEBUG is disabled, allows local users to cause a denial of service (memory corruption and crash) and possibly execute arbitrary code via an XFS image containing a symbolic link with a long pathname.
CVE-2011-4081	crypto/ghash-generic.c in the Linux kernel before 3.1 allows local users to cause a denial of service (NULL pointer dereference and OOPS) or possibly

	have unspecified other impact by triggering a failed or missing ghash_setkey function call, followed by a (1) ghash_update function call or (2) ghash_final function call, as demonstrated by a write operation on an AF_ALG socket.
CVE-2011-4086	The journal_unmap_buffer function in fs/jbd2/transaction.c in the Linux kernel before 3.3.1 does not properly handle the _Delay and _Unwritten buffer head states, which allows local users to cause a denial of service (system crash) by leveraging the presence of an ext4 filesystem that was mounted with a journal.
CVE-2011-4108	The DTLS implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f performs a MAC check only if certain padding is valid, which makes it easier for remote attackers to recover plaintext via a padding oracle attack.
CVE-2011-4110	The user_update function in security/keys/user_defined.c in the Linux kernel 2.6 allows local users to cause a denial of service (NULL pointer dereference and kernel oops) via vectors related to a user-defined key and "updating a negative key into a fully instantiated key."
CVE-2011-4127	The Linux kernel before 3.2.2 does not properly restrict SG_IO ioctl calls, which allows local users to bypass intended restrictions on disk read and write operations by sending a SCSI command to (1) a partition block device or (2) an LVM volume.
CVE-2011-4128	Buffer overflow in the gnutls_session_get_data function in lib/gnutls_session.c in GnuTLS 2.12.x before 2.12.14 and 3.x before 3.0.7, when used on a client that performs nonstandard session resumption, allows remote TLS servers to cause a denial of service (application crash) via a large SessionTicket.
CVE-2011-4131	The NFSv4 implementation in the Linux kernel before 3.2.2 does not properly handle bitmap sizes in GETACL replies, which allows remote NFS servers to cause a denial of service (OOPS) by sending an excessive number of bitmap words.
CVE-2011-4132	The cleanup_journal_tail function in the Journaling Block Device (JBD) functionality in the Linux kernel 2.6 allows local users to cause a denial of service (assertion error and kernel oops) via an ext3 or ext4 image with an "invalid log first block value."
CVE-2011-4313	query.c in ISC BIND 9.0.x through 9.6.x, 9.4-ESV through 9.4-ESV-R5, 9.6-ESV through 9.6-ESV-R5, 9.7.0 through 9.7.4, 9.8.0 through 9.8.1, and 9.9.0a1 through 9.9.0b1 allows remote attackers to cause a denial of service (assertion failure and named exit) via unknown vectors related to recursive DNS queries,

	error logging, and the caching of an invalid record by the resolver.
CVE-2011-4315	Heap-based buffer overflow in compression-pointer processing in core/ngx_resolver.c in nginx before 1.0.10 allows remote resolvers to cause a denial of service (daemon crash) or possibly have unspecified other impact via a long response.
CVE-2011-4326	The udp6_ufo_fragment function in net/ipv6/udp.c in the Linux kernel before 2.6.39, when a certain UDP Fragmentation Offload (UFO) configuration is enabled, allows remote attackers to cause a denial of service (system crash) by sending fragmented IPv6 UDP packets to a bridge device.
CVE-2011-4347	The kvm_vm_ioctl_assign_device function in virt/kvm/assigned-dev.c in the KVM subsystem in the Linux kernel before 3.1.10 does not verify permission to access PCI configuration space and BAR resources, which allows host OS users to assign PCI devices and cause a denial of service (host OS crash) via a KVM_ASSIGN_PCI_DEVICE operation.
CVE-2011-4355	GNU Project Debugger (GDB) before 7.5, when .debug_gdb_scripts is defined, automatically loads certain files from the current working directory, which allows local users to gain privileges via crafted files such as Python scripts.
CVE-2011-4362	Integer signedness error in the base64_decode function in the HTTP authentication functionality (http_auth.c) in lighttpd 1.4 before 1.4.30 and 1.5 before SVN revision 2806 allows remote attackers to cause a denial of service (segmentation fault) via crafted base64 input that triggers an out-of-bounds read with a negative index.
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-2011-4516	Heap-based buffer overflow in the jpc_cox_getcompparms function in libjasper/jpc/

	jpc_cs.c in JasPer 1.900.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted numrlvls value in a coding style default (COD) marker segment in a JPEG2000 file.
CVE-2011-4539	dhcpd in ISC DHCP 4.x before 4.2.3-P1 and 4.1-ESV before 4.1-ESV-R4 does not properly handle regular expressions in dhcpd.conf, which allows remote attackers to cause a denial of service (daemon crash) via a crafted request packet.
CVE-2011-4566	Integer overflow in the exif_process_IFD_TAG function in exif.c in the exif extension in PHP 5.4.0beta2 on 32-bit platforms allows remote attackers to read the contents of arbitrary memory locations or cause a denial of service via a crafted offset_val value in an EXIF header in a JPEG file, a different vulnerability than CVE-2011-0708.
CVE-2011-4576	The SSL 3.0 implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does not properly initialize data structures for block cipher padding, which might allow remote attackers to obtain sensitive information by decrypting the padding data sent by an SSL peer.
CVE-2011-4577	OpenSSL before 0.9.8s and 1.x before 1.0.0f, when RFC 3779 support is enabled, allows remote attackers to cause a denial of service (assertion failure) via an X.509 certificate containing certificate-extension data associated with (1) IP address blocks or (2) Autonomous System (AS) identifiers.
CVE-2011-4594	The __sys_sendmsg function in net/socket.c in the Linux kernel before 3.1 allows local users to cause a denial of service (system crash) via crafted use of the sendmmsg system call, leading to an incorrect pointer dereference.
CVE-2011-4599	Stack-based buffer overflow in the _canonicalize function in common/uloc.c in International Components for Unicode (ICU) before 49.1 allows remote attackers to execute arbitrary code via a crafted locale ID that is not properly handled during variant canonicalization.
CVE-2011-4609	The svc_run function in the RPC implementation in glibc before 2.15 allows remote attackers to cause a denial of service (CPU consumption) via a large number of RPC connections.
CVE-2011-4611	Integer overflow in the perf_event_interrupt function in arch/powerpc/kernel/perf_event.c in the Linux kernel before 2.6.39 on powerpc platforms allows local users to cause a denial of service (unhandled performance monitor exception) via vectors that trigger certain outcomes of performance events.
CVE-2011-4619	The Server Gated Cryptography (SGC) implementation in OpenSSL before 0.9.8s and 1.x before 1.0.0f does

	not properly handle handshake restarts, which allows remote attackers to cause a denial of service (CPU consumption) via unspecified vectors.
CVE-2011-4622	The create_pit_timer function in arch/x86/kvm/i8254.c in KVM 83, and possibly other versions, does not properly handle when Programmable Interval Timer (PIT) interrupt requests (IRQs) when a virtual interrupt controller (irqchip) is not available, which allows local users to cause a denial of service (NULL pointer dereference) by starting a timer.
CVE-2011-4623	Integer overflow in the rsCStrExtendBuf function in runtime/stringbuf.c in the imfile module in rsyslog 4.x before 4.6.6, 5.x before 5.7.4, and 6.x before 6.1.4 allows local users to cause a denial of service (daemon hang) via a large file, which triggers a heap-based buffer overflow.
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-2011-4718	Session fixation vulnerability in the Sessions subsystem in PHP before 5.5.2 allows remote attackers to hijack web sessions by specifying a session ID.
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-2011-4815	Ruby (aka CRuby) before 1.8.7-p357 computes hash values without restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted input to an application that maintains a hash table.
CVE-2011-4885	PHP before 5.3.9 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-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-2011-4940	The list_directory function in Lib/SimpleHTTPServer.py in SimpleHTTPServer in Python before 2.5.6c1, 2.6.x before 2.6.7 rc2, and 2.7.x before 2.7.2 does not place a charset parameter in the Content-Type HTTP header, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks against Internet Explorer 7 via UTF-7 encoding.

CVE-2011-4944	Python 2.6 through 3.2 creates ~/.pypirc with world-readable permissions before changing them after data has been written, which introduces a race condition that allows local users to obtain a username and password by reading this file.
CVE-2011-5000	The ssh_gssapi_parse_ename function in gss-serv.c in OpenSSH 5.8 and earlier, when gssapi-with-mic authentication is enabled, allows remote authenticated users to cause a denial of service (memory consumption) via a large value in a certain length field. NOTE: there may be limited scenarios in which this issue is relevant.
CVE-2011-5035	Oracle Glassfish 2.1.1, 3.0.1, and 3.1.1, as used in Communications Server 2.0, Sun Java System Application Server 8.1 and 8.2, and possibly other products, 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, aka Oracle security ticket S0104869.
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-2012-0031	scoreboard.c in the Apache HTTP Server 2.2.21 and earlier might allow local users to cause a denial of service (daemon crash during shutdown) or possibly have unspecified other impact by modifying a certain type field within a scoreboard shared memory segment, leading to an invalid call to the free function.
CVE-2012-0038	Integer overflow in the xfs_acl_from_disk function in fs/xfs/xfs_acl.c in the Linux kernel before 3.1.9 allows local users to cause a denial of service (panic) via a filesystem with a malformed ACL, leading to a heap-based buffer overflow.
CVE-2012-0045	The em_syscall function in arch/x86/kvm/emulate.c in the KVM implementation in the Linux kernel before 3.2.14 does not properly handle the 0f05 (aka syscall) opcode, which allows guest OS users to cause a denial of service (guest OS crash) via a crafted application, as demonstrated by an NASM file.
CVE-2012-0053	protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header information during construction of Bad Request (aka 400) error documents, which allows remote attackers to obtain the values of HTTPOnly cookies via vectors involving a (1)

	long or (2) malformed header in conjunction with crafted web script.
CVE-2012-0060	RPM before 4.9.1.3 does not properly validate region tags, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via an invalid region tag in a package header to the (1) headerLoad, (2) rpmReadSignature, or (3) headerVerify function.
CVE-2012-0075	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows remote authenticated users to affect integrity via unknown vectors.
CVE-2012-0087	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x and 5.1.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0101 and CVE-2012-0102.
CVE-2012-0101	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x and 5.1.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0087 and CVE-2012-0102.
CVE-2012-0112	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, CVE-2012-0485, and CVE-2012-0492.
CVE-2012-0113	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect confidentiality and availability via unknown vectors, a different vulnerability than CVE-2012-0118.
CVE-2012-0114	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows local users to affect confidentiality and integrity via unknown vectors.
CVE-2012-0115	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0119, CVE-2012-0120, CVE-2012-0485, and CVE-2012-0492.
CVE-2012-0116	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect confidentiality and integrity via unknown vectors.
CVE-2012-0118	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows

	remote authenticated users to affect confidentiality and availability via unknown vectors, a different vulnerability than CVE-2012-0113.
CVE-2012-0119	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0120, CVE-2012-0485, and CVE-2012-0492.
CVE-2012-0120	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0119, CVE-2012-0485, and CVE-2012-0492.
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-2012-0207	The igmp_heard_query function in net/ipv4/igmp.c in the Linux kernel before 3.2.1 allows remote attackers to cause a denial of service (divide-by-zero error and panic) via IGMP packets.
CVE-2012-0219	Heap-based buffer overflow in the xioscan_readline function in xio-readline.c in socat 1.4.0.0 through 1.7.2.0 and 2.0.0-b1 through 2.0.0-b4 allows local users to execute arbitrary code via the READLINE address.
CVE-2012-0247	ImageMagick 6.7.5-7 and earlier allows remote attackers to cause a denial of service (memory corruption) and possibly execute arbitrary code via crafted offset and count values in the ResolutionUnit tag in the EXIF IFD0 of an image.
CVE-2012-0248	ImageMagick 6.7.5-7 and earlier allows remote attackers to cause a denial of service (infinite loop and hang) via a crafted image whose IFD contains IOP tags that all reference the beginning of the IDF.
CVE-2012-0250	Buffer overflow in the OSPFv2 implementation in ospfd in Quagga before 0.99.20.1 allows remote attackers to cause a denial of service (daemon crash) via a Link State Update (aka LS Update) packet containing a network-LSA link-state advertisement for which the data-structure length is smaller than the value in the Length header field.

CVE-2012-0259	The GetEXIFProperty function in magick/property.c in ImageMagick before 6.7.6-3 allows remote attackers to cause a denial of service (crash) via a zero value in the component count of an EXIF XResolution tag in a JPEG file, which triggers an out-of-bounds read.
CVE-2012-0260	The JPEGWarningHandler function in coders/jpeg.c in ImageMagick before 6.7.6-3 allows remote attackers to cause a denial of service (memory consumption) via a JPEG image with a crafted sequence of restart markers.
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-2012-0441	The ASN.1 decoder in the QuickDER decoder in Mozilla Network Security Services (NSS) before 3.13.4, as used in Firefox 4.x through 12.0, Firefox ESR 10.x before 10.0.5, Thunderbird 5.0 through 12.0, Thunderbird ESR 10.x before 10.0.5, and SeaMonkey before 2.10, allows remote attackers to cause a denial of service (application crash) via a zero-length item, as demonstrated by (1) a zero-length basic constraint or (2) a zero-length field in an OCSP response.
CVE-2012-0444	Mozilla Firefox before 3.6.26 and 4.x through 9.0, Thunderbird before 3.1.18 and 5.0 through 9.0, and SeaMonkey before 2.7 do not properly initialize nsChildView data structures, which allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via a crafted Ogg Vorbis file.
CVE-2012-0484	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and

	5.5.x allows remote authenticated users to affect confidentiality via unknown vectors.
CVE-2012-0485	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, and CVE-2012-0492.
CVE-2012-0490	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.0.x, 5.1.x, and 5.5.x allows remote authenticated users to affect availability via unknown vectors.
CVE-2012-0492	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.x and 5.5.x allows remote authenticated users to affect availability via unknown vectors, a different vulnerability than CVE-2012-0112, CVE-2012-0115, CVE-2012-0119, CVE-2012-0120, and CVE-2012-0485.
CVE-2012-0497	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, and 6 Update 30 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.
CVE-2012-0501	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, and 5.0 Update 33 and earlier allows remote attackers to affect availability via unknown vectors.
CVE-2012-0502	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, 5.0 Update 33 and earlier, and 1.4.2_35 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect confidentiality and availability, related to AWT.
CVE-2012-0503	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, 5.0 Update 33 and earlier, and 1.4.2_35 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect confidentiality, integrity, and availability, related to I18n.
CVE-2012-0505	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, 5 Update 33 and earlier, and 1.4.2_35 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect confidentiality, integrity, and availability via unknown vectors related to Serialization.

CVE-2012-0506	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 2 and earlier, 6 Update 30 and earlier, 5.0 Update 33 and earlier, and 1.4.2_35 and earlier allows remote untrusted Java Web Start applications and untrusted Java applets to affect integrity via unknown vectors related to CORBA.
CVE-2012-0547	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 6 and earlier, and 6 Update 34 and earlier, has no impact and remote attack vectors involving AWT and "a security-in-depth issue that is not directly exploitable but which can be used to aggravate security vulnerabilities that can be directly exploited." NOTE: this identifier was assigned by the Oracle CNA, but CVE is not intended to cover defense-in-depth issues that are only exposed by the presence of other vulnerabilities. NOTE: Oracle has not commented on claims from a downstream vendor that this issue is related to "toolkit internals references."
CVE-2012-0572	Unspecified vulnerability in the Server component in Oracle MySQL 5.1.66 and earlier and 5.5.28 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.
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-2012-0786	The transform_save function in transform.c in Augeas before 1.0.0 allows local users to overwrite arbitrary files and obtain sensitive information via a symlink attack on a .augnew file.
CVE-2012-0787	The clone_file function in transfer.c in Augeas before 1.0.0, when copy_if_rename_fails is set and EXDEV or EBUSY is returned by the rename function, allows local users to overwrite arbitrary files and obtain sensitive information via a bind mount on the (1) .augsave or (2) destination file when using the backup save option, or (3) .augnew file when using the newfile save option.
CVE-2012-0804	Heap-based buffer overflow in the proxy_connect function in src/client.c in CVS 1.11 and 1.12 allows remote HTTP proxy servers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted HTTP response.
CVE-2012-0830	The php_register_variable_ex function in php_variables.c in PHP 5.3.9 allows remote attackers to execute arbitrary code via a request containing a large number of variables, related to improper handling of array variables. NOTE: this vulnerability exists because of an incorrect fix for CVE-2011-4885.
CVE-2012-0841	libxml2 before 2.8.0 computes hash values without restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted XML data.
CVE-2012-0845	SimpleXMLRPCServer.py in SimpleXMLRPCServer in Python before 2.6.8, 2.7.x before 2.7.3, 3.x before 3.1.5, and 3.2.x before 3.2.3 allows remote attackers

	to cause a denial of service (infinite loop and CPU consumption) via an XML-RPC POST request that contains a smaller amount of data than specified by the Content-Length header.
CVE-2012-0864	Integer overflow in the vfprintf function in stdio-common/vfprintf.c in glibc 2.14 and other versions allows context-dependent attackers to bypass the FORTIFY_SOURCE protection mechanism, conduct format string attacks, and write to arbitrary memory via a large number of arguments.
CVE-2012-0866	CREATE TRIGGER in PostgreSQL 8.3.x before 8.3.18, 8.4.x before 8.4.11, 9.0.x before 9.0.7, and 9.1.x before 9.1.3 does not properly check the execute permission for trigger functions marked SECURITY DEFINER, which allows remote authenticated users to execute otherwise restricted triggers on arbitrary data by installing the trigger on an attacker-owned table.
CVE-2012-0867	PostgreSQL 8.4.x before 8.4.11, 9.0.x before 9.0.7, and 9.1.x before 9.1.3 truncates the common name to only 32 characters when verifying SSL certificates, which allows remote attackers to spoof connections when the host name is exactly 32 characters.
CVE-2012-0868	CRLF injection vulnerability in pg_dump in PostgreSQL 8.3.x before 8.3.18, 8.4.x before 8.4.11, 9.0.x before 9.0.7, and 9.1.x before 9.1.3 allows user-assisted remote attackers to execute arbitrary SQL commands via a crafted file containing object names with newlines, which are inserted into an SQL script that is used when the database is restored.
CVE-2012-0875	SystemTap 1.7, 1.6.7, and probably other versions, when unprivileged mode is enabled, allows local users to obtain sensitive information from kernel memory or cause a denial of service (kernel panic and crash) via vectors related to crafted DWARF data, which triggers a read of an invalid pointer.
CVE-2012-0876	The XML parser (xmlparse.c) in expat before 2.1.0 computes hash values without restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via an XML file with many identifiers with the same value.
CVE-2012-0884	The implementation of Cryptographic Message Syntax (CMS) and PKCS #7 in OpenSSL before 0.9.8u and 1.x before 1.0.0h does not properly restrict certain oracle behavior, which makes it easier for context-dependent attackers to decrypt data via a Million Message Attack (MMA) adaptive chosen ciphertext attack.
CVE-2012-0946	The NVIDIA UNIX driver before 295.40 allows local users to access arbitrary memory locations by leveraging GPU device-node read/write privileges.

CVE-2012-0957	The override_release function in kernel/sys.c in the Linux kernel before 3.4.16 allows local users to obtain sensitive information from kernel stack memory via a uname system call in conjunction with a UNAME26 personality.
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-2012-1013	The check_1_6_dummy function in lib/kadm5/srv/svr_principal.c in kadmind in MIT Kerberos 5 (aka krb5) 1.8.x, 1.9.x, and 1.10.x before 1.10.2 allows remote authenticated administrators to cause a denial of service (NULL pointer dereference and daemon crash) via a KRB5_KDB_DISALLOW_ALL_TIX create request that lacks a password.
CVE-2012-1015	The kdc_handle_protected_negotiation function in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.8.x, 1.9.x before 1.9.5, and 1.10.x before 1.10.3 attempts to calculate a checksum before verifying that the key type is appropriate for a checksum, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free, heap memory corruption, and daemon crash) via a crafted AS-REQ request.
CVE-2012-1033	The resolver in ISC BIND 9 through 9.8.1-P1 overwrites cached server names and TTL values in NS records during the processing of a response to an A record query, which allows remote attackers to trigger continued resolvability of revoked domain names via a "ghost domain names" attack.
CVE-2012-1053	The change_user method in the SUIDManager (lib/puppet/util/suidmanager.rb) in Puppet 2.6.x before 2.6.14 and 2.7.x before 2.7.11, and Puppet Enterprise (PE) Users 1.0, 1.1, 1.2.x, 2.0.x before 2.0.3 does not properly manage group privileges, which allows local users to gain privileges via vectors related to (1) the change_user not dropping supplementary groups in certain conditions, (2) changes to the eguid without associated changes to the egid, or (3) the addition of the real gid to supplementary groups.
CVE-2012-1054	Puppet 2.6.x before 2.6.14 and 2.7.x before 2.7.11, and Puppet Enterprise (PE) Users 1.0, 1.1, 1.2.x, 2.0.x before 2.0.3, when managing a user login file with the k5login resource type, allows local users to gain privileges via a symlink attack on .k5login.

CVE-2012-1088	iproute2 before 3.3.0 allows local users to overwrite arbitrary files via a symlink attack on a temporary file used by (1) configure or (2) examples/dhcp-client-script.
CVE-2012-1126	FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap read operation and memory corruption) or possibly execute arbitrary code via crafted property data in a BDF font.
CVE-2012-1134	FreeType before 2.4.9, as used in Mozilla Firefox Mobile before 10.0.4 and other products, allows remote attackers to cause a denial of service (invalid heap write operation and memory corruption) or possibly execute arbitrary code via crafted private-dictionary data in a Type 1 font.
CVE-2012-1148	Memory leak in the poolGrow function in expat/lib/xmlparse.c in expat before 2.1.0 allows context-dependent attackers to cause a denial of service (memory consumption) via a large number of crafted XML files that cause improperly-handled reallocation failures when expanding entities.
CVE-2012-1150	Python before 2.6.8, 2.7.x before 2.7.3, 3.x before 3.1.5, and 3.2.x before 3.2.3 computes hash values without restricting the ability to trigger hash collisions predictably, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted input to an application that maintains a hash table.
CVE-2012-1151	Multiple format string vulnerabilities in dbdimp.c in DBD::Pg (aka DBD-Pg or libdbd-pg-perl) module before 2.19.0 for Perl allow remote PostgreSQL database servers to cause a denial of service (process crash) via format string specifiers in (1) a crafted database warning to the pg_warn function or (2) a crafted DBD statement to the dbd_st_prepare function.
CVE-2012-1152	Multiple format string vulnerabilities in the error reporting functionality in the YAML::LibYAML (aka YAML-LibYAML and perl-YAML-LibYAML) module 0.38 for Perl allow remote attackers to cause a denial of service (process crash) via format string specifiers in a (1) YAML stream to the Load function, (2) YAML node to the load_node function, (3) YAML mapping to the load_mapping function, or (4) YAML sequence to the load_sequence function.
CVE-2012-1164	slapd in OpenLDAP before 2.4.30 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via an LDAP search query with attrsOnly set to true, which causes empty attributes to be returned.
CVE-2012-1165	The mime_param_cmp function in crypto/asn1/asn_mime.c in OpenSSL before 0.9.8u and 1.x before

	1.0.0h allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted S/MIME message, a different vulnerability than CVE-2006-7250.
CVE-2012-1173	Multiple integer overflows in tiff_getimage.c in LibTIFF 3.9.4 allow remote attackers to execute arbitrary code via a crafted tile size in a TIFF file, which is not properly handled by the (1) gtTileSeparate or (2) gtStripSeparate function, leading to a heap-based buffer overflow.
CVE-2012-1180	Use-after-free vulnerability in nginx before 1.0.14 and 1.1.x before 1.1.17 allows remote HTTP servers to obtain sensitive information from process memory via a crafted backend response, in conjunction with a client request.
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-2012-1568	The ExecShield feature in a certain Red Hat patch for the Linux kernel in Red Hat Enterprise Linux (RHEL) 5 and 6 and Fedora 15 and 16 does not properly handle use of many shared libraries by a 32-bit executable file, which makes it easier for context-dependent attackers to bypass the ASLR protection mechanism by leveraging a predictable base address for one of these libraries.
CVE-2012-1569	The asn1_get_length_der function in decoding.c in GNU Libtasn1 before 2.12, as used in GnuTLS before 3.0.16 and other products, does not properly handle certain large length values, which allows remote attackers to cause a denial of service (heap memory

	corruption and application crash) or possibly have unspecified other impact via a crafted ASN.1 structure.
CVE-2012-1571	file before 5.11 and libmagic allow remote attackers to cause a denial of service (crash) via a crafted Composite Document File (CDF) file that triggers (1) an out-of-bounds read or (2) an invalid pointer dereference.
CVE-2012-1573	gnutls_cipher.c in libgnutls in GnuTLS before 2.12.17 and 3.x before 3.0.15 does not properly handle data encrypted with a block cipher, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) via a crafted record, as demonstrated by a crafted GenericBlockCipher structure.
CVE-2012-1667	ISC BIND 9.x before 9.7.6-P1, 9.8.x before 9.8.3-P1, 9.9.x before 9.9.1-P1, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P1 does not properly handle resource records with a zero-length RDATA section, which allows remote DNS servers to cause a denial of service (daemon crash or data corruption) or obtain sensitive information from process memory via a crafted record.
CVE-2012-1682	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 6 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Beans, a different vulnerability than CVE-2012-3136. NOTE: Oracle has not commented on claims from a downstream vendor that this issue is related to "XMLDecoder security issue via ClassFinder."
CVE-2012-1688	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.61 and earlier, and 5.5.21 and earlier, allows remote authenticated users to affect availability, related to Server DML.
CVE-2012-1711	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 update 4 and earlier, 6 update 32 and earlier, 5 update 35 and earlier, and 1.4.2_37 and earlier allows remote attackers to affect confidentiality, integrity, and availability, related to CORBA.
CVE-2012-1713	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 update 4 and earlier, 6 update 32 and earlier, 5 update 35 and earlier, 1.4.2_37 and earlier, and JavaFX 2.1 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.
CVE-2012-1716	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 update 4 and earlier, 6 update 32 and earlier, and 5 update 35 and earlier allows remote attackers to affect

	confidentiality, integrity, and availability via unknown vectors related to Swing.
CVE-2012-1717	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 update 4 and earlier, 6 update 32 and earlier, 5 update 35 and earlier, and 1.4.2_37 and earlier allows local users to affect confidentiality via unknown vectors related to printing on Solaris or Linux.
CVE-2012-1718	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 update 4 and earlier, 6 update 32 and earlier, 5 update 35 and earlier, and 1.4.2_37 and earlier allows remote attackers to affect availability via unknown vectors related to Security.
CVE-2012-1723	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 update 4 and earlier, 6 update 32 and earlier, 5 update 35 and earlier, and 1.4.2_37 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot.
CVE-2012-1724	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 update 4 and earlier, and 6 update 32 and earlier, allows remote attackers to affect availability, related to JAXP.
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-2012-1798	The TIFFGetEXIFProperties function in coders/tiff.c in ImageMagick before 6.7.6-3 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted EXIF IFD in a TIFF image.
CVE-2012-1820	The bgp_capability_orf function in bgpd in Quagga 0.99.20.1 and earlier allows remote attackers to cause a denial of service (assertion failure and daemon exit) by leveraging a BGP peering relationship and sending a malformed Outbound Route Filtering (ORF) capability TLV in an OPEN message.
CVE-2012-1823	sapi/cgi/cgi_main.c in PHP before 5.3.12 and 5.4.x before 5.4.2, when configured as a CGI script (aka php-cgi), does not properly handle query strings that lack an = (equals sign) character, which allows remote attackers to execute arbitrary code by placing command-line options in the query string, related to lack of skipping a certain php_getopt for the 'd' case.

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-2012-1986	Puppet 2.6.x before 2.6.15 and 2.7.x before 2.7.13, and Puppet Enterprise (PE) Users 1.0, 1.1, 1.2.x, 2.0.x, and 2.5.x before 2.5.1 allows remote authenticated users with an authorized SSL key and certain permissions on the puppet master to read arbitrary files via a symlink attack in conjunction with a crafted REST request for a file in a filebucket.
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-2012-2088	Integer signedness error in the TIFFReadDirectory function in tif_dirread.c in libtiff 3.9.4 and earlier allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a negative tile depth in a tiff image, which triggers an improper conversion between signed and unsigned types, leading to a heap-based buffer overflow.
CVE-2012-2089	Buffer overflow in ngx_http_mp4_module.c in the ngx_http_mp4_module module in nginx 1.0.7 through 1.0.14 and 1.1.3 through 1.1.18, when the mp4 directive is used, allows remote attackers to cause a denial of service (memory overwrite) or possibly execute arbitrary code via a crafted MP4 file.
CVE-2012-2100	The ext4_fill_flex_info function in fs/ext4/super.c in the Linux kernel before 3.2.2, on the x86 platform and unspecified other platforms, allows user-assisted remote attackers to trigger inconsistent filesystem-groups data and possibly cause a denial of service via a malformed ext4 filesystem containing a super block with a large FLEX_BG group size (aka s_log_groups_per_flex value). NOTE: this vulnerability exists because of an incomplete fix for CVE-2009-4307.
CVE-2012-2102	MySQL 5.1.x before 5.1.62 and 5.5.x before 5.5.22 allows remote authenticated users to cause a denial of service (assertion failure and mysqld abort) by deleting a record and using HANDLER READ NEXT.
CVE-2012-2110	The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.
CVE-2012-2113	Multiple integer overflows in tiff2pdf in libtiff before 4.0.2 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tiff image, which triggers a heap-based buffer overflow.
CVE-2012-2122	sql/password.c in Oracle MySQL 5.1.x before 5.1.63, 5.5.x before 5.5.24, and 5.6.x before 5.6.6, and MariaDB 5.1.x before 5.1.62, 5.2.x before 5.2.12, 5.3.x

	before 5.3.6, and 5.5.x before 5.5.23, when running in certain environments with certain implementations of the memcmp function, allows remote attackers to bypass authentication by repeatedly authenticating with the same incorrect password, which eventually causes a token comparison to succeed due to an improperly-checked return value.
CVE-2012-2125	RubyGems before 1.8.23 can redirect HTTPS connections to HTTP, which makes it easier for remote attackers to observe or modify a gem during installation via a man-in-the-middle attack.
CVE-2012-2133	Use-after-free vulnerability in the Linux kernel before 3.3.6, when huge pages are enabled, allows local users to cause a denial of service (system crash) or possibly gain privileges by interacting with a hugetlbfs filesystem, as demonstrated by a umount operation that triggers improper handling of quota data.
CVE-2012-2136	The sock_alloc_send_pskb function in net/core/sock.c in the Linux kernel before 3.4.5 does not properly validate a certain length value, which allows local users to cause a denial of service (heap-based buffer overflow and system crash) or possibly gain privileges by leveraging access to a TUN/TAP device.
CVE-2012-2141	Array index error in the handle_nsExtendOutput2Table function in agent/mibgroup/agent/extend.c in Net-SNMP 5.7.1 allows remote authenticated users to cause a denial of service (out-of-bounds read and snmpd crash) via an SNMP GET request for an entry not in the extension table.
CVE-2012-2143	The crypt_des (aka DES-based crypt) function in FreeBSD before 9.0-RELEASE-p2, as used in PHP, PostgreSQL, and other products, does not process the complete cleartext password if this password contains a 0x80 character, which makes it easier for context-dependent attackers to obtain access via an authentication attempt with an initial substring of the intended password, as demonstrated by a Unicode password.
CVE-2012-2150	xfs_metadump in xfsprogs before 3.2.4 does not properly obfuscate file data, which allows remote attackers to obtain sensitive information by reading a generated image.
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-2012-2313	The rio_ioctl function in drivers/net/ethernet/dlink/dl2k.c in the Linux kernel before 3.3.7 does not restrict access to the SIOCSMIIREG command, which allows local users to write data to an Ethernet adapter via an ioctl call.
CVE-2012-2333	Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation.
CVE-2012-2337	sudo 1.6.x and 1.7.x before 1.7.9p1, and 1.8.x before 1.8.4p5, does not properly support configurations that use a netmask syntax, which allows local users to bypass intended command restrictions in opportunistic circumstances by executing a command on a host that has an IPv4 address.
CVE-2012-2372	The rds_ib_xmit function in net/rds/ib_send.c in the Reliable Datagram Sockets (RDS) protocol implementation in the Linux kernel 3.7.4 and earlier allows local users to cause a denial of service (BUG_ON and kernel panic) by establishing an RDS connection with the source IP address equal to the IPoIB interface's own IP address, as demonstrated by rds-ping.
CVE-2012-2375	The __nfs4_get_acl_uncached function in fs/nfs/nfs4proc.c in the NFSv4 implementation in the Linux kernel before 3.3.2 uses an incorrect length variable during a copy operation, which allows remote NFS servers to cause a denial of service (OOPS) by sending an excessive number of bitmap words in an

	FATTR4_ACL reply. NOTE: this vulnerability exists because of an incomplete fix for CVE-2011-4131.
CVE-2012-2384	Integer overflow in the i915_gem_do_execbuffer function in drivers/gpu/drm/i915/i915_gem_execbuffer.c in the Direct Rendering Manager (DRM) subsystem in the Linux kernel before 3.3.5 on 32-bit platforms allows local users to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via a crafted ioctl call.
CVE-2012-2386	Integer overflow in the phar_parse_tarfile function in tar.c in the phar extension in PHP before 5.3.14 and 5.4.x before 5.4.4 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted tar file that triggers a heap-based buffer overflow.
CVE-2012-2390	Memory leak in mm/hugetlb.c in the Linux kernel before 3.4.2 allows local users to cause a denial of service (memory consumption or system crash) via invalid MAP_HUGETLB mmap operations.
CVE-2012-2392	Wireshark 1.4.x before 1.4.13 and 1.6.x before 1.6.8 allows remote attackers to cause a denial of service (infinite loop) via vectors related to the (1) ANSI MAP, (2) ASF, (3) IEEE 802.11, (4) IEEE 802.3, and (5) LTP dissectors.
CVE-2012-2417	PyCrypto before 2.6 does not produce appropriate prime numbers when using an ElGamal scheme to generate a key, which reduces the signature space or public key space and makes it easier for attackers to conduct brute force attacks to obtain the private key.
CVE-2012-2655	PostgreSQL 8.3.x before 8.3.19, 8.4.x before 8.4.12, 9.0.x before 9.0.8, and 9.1.x before 9.1.4 allows remote authenticated users to cause a denial of service (server crash) by adding the (1) SECURITY DEFINER or (2) SET attributes to a procedural language's call handler.
CVE-2012-2668	libraries/libldap/tls_m.c in OpenLDAP, possibly 2.4.31 and earlier, when using the Mozilla NSS backend, always uses the default cipher suite even when TLSCipherSuite is set, which might cause OpenLDAP to use weaker ciphers than intended and make it easier for remote attackers to obtain sensitive information.
CVE-2012-2673	Multiple integer overflows in the (1) GC_generic_malloc and (2) calloc functions in malloc.c, and the (3) GC_generic_malloc_ignore_off_page function in mallocx.c in Boehm-Demers-Weiser GC (libgc) before 7.2 make it easier for context-dependent attackers to perform memory-related attacks such as buffer overflows via a large size value, which causes less memory to be allocated than expected.
CVE-2012-2688	Unspecified vulnerability in the _php_stream_scandir function in the stream implementation in PHP before

	5.3.15 and 5.4.x before 5.4.5 has unknown impact and remote attack vectors, related to an "overflow."
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-2012-2812	The exif_entry_get_value function in exif-entry.c in the EXIF Tag Parsing Library (aka libexif) before 0.6.21 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly obtain sensitive information from process memory via crafted EXIF tags in an image.
CVE-2012-2813	The exif_convert_utf16_to_utf8 function in exif-entry.c in the EXIF Tag Parsing Library (aka libexif) before 0.6.21 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly obtain sensitive information from process memory via crafted EXIF tags in an image.
CVE-2012-2814	Buffer overflow in the exif_entry_format_value function in exif-entry.c in the EXIF Tag Parsing Library (aka libexif) 0.6.20 allows remote attackers to cause a denial of service or possibly execute arbitrary code via crafted EXIF tags in an image.
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-2012-2836	The exif_data_load_data function in exif-data.c in the EXIF Tag Parsing Library (aka libexif) before 0.6.21 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly obtain sensitive information from process memory via crafted EXIF tags in an image.
CVE-2012-2837	The mnote_olympus_entry_get_value function in olympus/mnote-olympus-entry.c in the EXIF Tag Parsing Library (aka libexif) before 0.6.21 allows remote attackers to cause a denial of service (divide-by-zero error) via an image with crafted EXIF tags that are not properly handled during the formatting of EXIF maker note tags.
CVE-2012-2840	Off-by-one error in the exif_convert_utf16_to_utf8 function in exif-entry.c in the EXIF Tag Parsing Library (aka libexif) before 0.6.21 allows remote attackers to cause a denial of service or possibly execute arbitrary code via crafted EXIF tags in an image.
CVE-2012-2841	Integer underflow in the exif_entry_get_value function in exif-entry.c in the EXIF Tag Parsing Library (aka libexif) 0.6.20 might allow remote attackers to execute arbitrary code via vectors involving a crafted buffer-size parameter during the formatting of an EXIF tag, leading to a heap-based buffer overflow.
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-2012-3174	Unspecified vulnerability in Oracle Java 7 before Update 11 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors, a different vulnerability than CVE-2013-0422. NOTE: some parties have mapped CVE-2012-3174 to an issue involving recursive use of the Reflection API, but that issue is already covered as part of CVE-2013-0422. This identifier is for a different vulnerability whose details are not public as of 20130114.
CVE-2012-3216	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, 6 Update 35 and earlier, 5.0 Update 36 and earlier, and 1.4.2_38 and earlier allows

	remote attackers to affect confidentiality via unknown vectors related to Libraries.
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-2012-3358	Multiple heap-based buffer overflows in the j2k_read_sot function in j2k.c in OpenJPEG 1.5 allow remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted (1) tile number or (2) tile length in a JPEG 2000 image file.
CVE-2012-3386	The "make distcheck" rule in GNU Automake before 1.11.6 and 1.12.x before 1.12.2 grants world-writable permissions to the extraction directory, which introduces a race condition that allows local users to execute arbitrary code via unspecified vectors.
CVE-2012-3400	Heap-based buffer overflow in the udf_load_logicalvol function in fs/udf/super.c in the Linux kernel before 3.4.5 allows remote attackers to cause a denial of service (system crash) or possibly have unspecified other impact via a crafted UDF filesystem.
CVE-2012-3401	The t2p_read_tiff_init function in tiff2pdf (tools/tiff2pdf.c) in LibTIFF 4.0.2 and earlier does not properly initialize the T2P context struct pointer in certain error conditions, which allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted TIFF image that triggers a heap-based buffer overflow.
CVE-2012-3404	The vfprintf function in stdio-common/vfprintf.c in libc in GNU C Library (aka glibc) 2.12 and other versions does not properly calculate a buffer length, which allows context-dependent attackers to bypass the FORTIFY_SOURCE format-string protection mechanism and cause a denial of service (stack corruption and crash) via a format string that uses positional parameters and many format specifiers.
CVE-2012-3405	The vfprintf function in stdio-common/vfprintf.c in libc in GNU C Library (aka glibc) 2.14 and other versions does not properly calculate a buffer length, which allows context-dependent attackers to bypass the FORTIFY_SOURCE format-string protection mechanism and cause a denial of service (segmentation fault and crash) via a format string with a large number of format specifiers that triggers "desynchronization within the buffer size handling," a different vulnerability than CVE-2012-3404.
CVE-2012-3406	The vfprintf function in stdio-common/vfprintf.c in GNU C Library (aka glibc) 2.5, 2.12, and probably other versions does not "properly restrict the use of" the

	alloca function when allocating the SPECS array, which allows context-dependent attackers to bypass the FORTIFY_SOURCE format-string protection mechanism and cause a denial of service (crash) or possibly execute arbitrary code via a crafted format string using positional parameters and a large number of format specifiers, a different vulnerability than CVE-2012-3404 and CVE-2012-3405.
CVE-2012-3411	Dnsmasq before 2.63test1, when used with certain libvirt configurations, replies to requests from prohibited interfaces, which allows remote attackers to cause a denial of service (traffic amplification) via a spoofed DNS query.
CVE-2012-3430	The rds_recvmsg function in net/rds/recv.c in the Linux kernel before 3.0.44 does not initialize a certain structure member, which allows local users to obtain potentially sensitive information from kernel stack memory via a (1) recvfrom or (2) recvmsg system call on an RDS socket.
CVE-2012-3480	Multiple integer overflows in the (1) strtod, (2) strtof, (3) strtold, (4) strtod_l, and other unspecified "related functions" in stdlib in GNU C Library (aka glibc or libc6) 2.16 allow local users to cause a denial of service (application crash) and possibly execute arbitrary code via a long string, which triggers a stack-based buffer overflow.
CVE-2012-3482	Fetchmail 5.0.8 through 6.3.21, when using NTLM authentication in debug mode, allows remote NTLM servers to (1) cause a denial of service (crash and delayed delivery of inbound mail) via a crafted NTLM response that triggers an out-of-bounds read in the base64 decoder, or (2) obtain sensitive information from memory via an NTLM Type 2 message with a crafted Target Name structure, which triggers an out-of-bounds read.
CVE-2012-3488	The libxslt support in contrib/xml2 in PostgreSQL 8.3 before 8.3.20, 8.4 before 8.4.13, 9.0 before 9.0.9, and 9.1 before 9.1.5 does not properly restrict access to files and URLs, which allows remote authenticated users to modify data, obtain sensitive information, or trigger outbound traffic to arbitrary external hosts by leveraging (1) stylesheet commands that are permitted by the libxslt security options or (2) an xslt_process feature, related to an XML External Entity (aka XXE) issue.
CVE-2012-3489	The xml_parse function in the libxml2 support in the core server component in PostgreSQL 8.3 before 8.3.20, 8.4 before 8.4.13, 9.0 before 9.0.9, and 9.1 before 9.1.5 allows remote authenticated users to determine the existence of arbitrary files or URLs, and possibly obtain file or URL content that triggers a

	parsing error, via an XML value that refers to (1) a DTD or (2) an entity, related to an XML External Entity (aka XXE) issue.
CVE-2012-3499	Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostnames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.
CVE-2012-3511	Multiple race conditions in the madvise_remove function in mm/madvise.c in the Linux kernel before 3.4.5 allow local users to cause a denial of service (use-after-free and system crash) via vectors involving a (1) munmap or (2) close system call.
CVE-2012-3512	Munin before 2.0.6 stores plugin state files that run as root in the same group-writable directory as non-root plugins, which allows local users to execute arbitrary code by replacing a state file, as demonstrated using the smart_ plugin.
CVE-2012-3520	The Netlink implementation in the Linux kernel before 3.2.30 does not properly handle messages that lack SCM_CREDENTIALS data, which might allow local users to spoof Netlink communication via a crafted message, as demonstrated by a message to (1) Avahi or (2) NetworkManager.
CVE-2012-3524	libdbus 1.5.x and earlier, when used in setuid or other privileged programs in X.org and possibly other products, allows local users to gain privileges and execute arbitrary code via the DBUS_SYSTEM_BUS_ADDRESS environment variable. NOTE: libdbus maintainers state that this is a vulnerability in the applications that do not cleanse environment variables, not in libdbus itself: "we do not support use of libdbus in setuid binaries that do not sanitize their environment before their first call into libdbus."
CVE-2012-3535	Heap-based buffer overflow in OpenJPEG 1.5.0 and earlier allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted JPEG2000 file.
CVE-2012-3544	Apache Tomcat 6.x before 6.0.37 and 7.x before 7.0.30 does not properly handle chunk extensions in chunked transfer coding, which allows remote attackers to cause a denial of service by streaming data.
CVE-2012-3547	Stack-based buffer overflow in the cbtls_verify function in FreeRADIUS 2.1.10 through 2.1.12, when using TLS-based EAP methods, allows remote attackers to cause a denial of service (server crash) and possibly execute

	arbitrary code via a long "not after" timestamp in a client certificate.
CVE-2012-3552	Race condition in the IP implementation in the Linux kernel before 3.0 might allow remote attackers to cause a denial of service (slab corruption and system crash) by sending packets to an application that sets socket options during the handling of network traffic.
CVE-2012-3571	ISC DHCP 4.1.2 through 4.2.4 and 4.1-ESV before 4.1-ESV-R6 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a malformed client identifier.
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-2012-3817	ISC BIND 9.4.x, 9.5.x, 9.6.x, and 9.7.x before 9.7.6-P2; 9.8.x before 9.8.3-P2; 9.9.x before 9.9.1-P2; and 9.6-ESV before 9.6-ESV-R7-P2, when DNSSEC validation is enabled, does not properly initialize the failing-query cache, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) by sending many queries.
CVE-2012-3825	Multiple integer overflows in Wireshark 1.4.x before 1.4.13 and 1.6.x before 1.6.8 allow remote attackers to cause a denial of service (infinite loop) via vectors related to the (1) BACapp and (2) Bluetooth HCI dissectors, a different vulnerability than CVE-2012-2392.
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-2012-3864	Puppet before 2.6.17 and 2.7.x before 2.7.18, and Puppet Enterprise before 2.5.2, allows remote authenticated users to read arbitrary files on the puppet master server by leveraging an arbitrary user's certificate and private key in a GET request.
CVE-2012-3865	Directory traversal vulnerability in lib/puppet/reports/store.rb in Puppet before 2.6.17 and 2.7.x before 2.7.18, and Puppet Enterprise before 2.5.2, when Delete is enabled in auth.conf, allows remote

	authenticated users to delete arbitrary files on the puppet master server via a .. (dot dot) in a node name.
CVE-2012-3866	lib/puppet/defaults.rb in Puppet 2.7.x before 2.7.18, and Puppet Enterprise before 2.5.2, uses 0644 permissions for last_run_report.yaml, which allows local users to obtain sensitive configuration information by leveraging access to the puppet master server to read this file.
CVE-2012-3867	lib/puppet/ssl/certificate_authority.rb in Puppet before 2.6.17 and 2.7.x before 2.7.18, and Puppet Enterprise before 2.5.2, does not properly restrict the characters in the Common Name field of a Certificate Signing Request (CSR), which makes it easier for user-assisted remote attackers to trick administrators into signing a crafted agent certificate via ANSI control sequences.
CVE-2012-3954	Multiple memory leaks in ISC DHCP 4.1.x and 4.2.x before 4.2.4-P1 and 4.1-ESV before 4.1-ESV-R6 allow remote attackers to cause a denial of service (memory consumption) by sending many requests.
CVE-2012-3955	ISC DHCP 4.1.x before 4.1-ESV-R7 and 4.2.x before 4.2.4-P2 allows remote attackers to cause a denial of service (daemon crash) in opportunistic circumstances by establishing an IPv6 lease in an environment where the lease expiration time is later reduced.
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-2012-4244	ISC BIND 9.x before 9.7.6-P3, 9.8.x before 9.8.3-P3, 9.9.x before 9.9.1-P3, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P3 allows remote attackers to cause a denial of service (assertion failure and named daemon exit) via a query for a long resource record.
CVE-2012-4285	The dissect_pft function in epan/dissectors/packet-dcp-etsi.c in the DCP ETSI dissector in Wireshark 1.4.x before 1.4.15, 1.6.x before 1.6.10, and 1.8.x before 1.8.2 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a zero-length message.
CVE-2012-4288	Integer overflow in the dissect_xtp_ecntl function in epan/dissectors/packet-xtp.c in the XTP dissector in Wireshark 1.4.x before 1.4.15, 1.6.x before 1.6.10, and 1.8.x before 1.8.2 allows remote attackers to cause a denial of service (loop or application crash) via a large value for a span length.
CVE-2012-4289	epan/dissectors/packet-afp.c in the AFP dissector in Wireshark 1.4.x before 1.4.15, 1.6.x before 1.6.10, and 1.8.x before 1.8.2 allows remote attackers to cause a denial of service (loop and CPU consumption) via a large number of ACL entries.
CVE-2012-4290	The CTDB dissector in Wireshark 1.4.x before 1.4.15, 1.6.x before 1.6.10, and 1.8.x before 1.8.2 allows remote attackers to cause a denial of service (loop and CPU consumption) via a malformed packet.
CVE-2012-4291	The CIP dissector in Wireshark 1.4.x before 1.4.15, 1.6.x before 1.6.10, and 1.8.x before 1.8.2 allows remote attackers to cause a denial of service (memory consumption) via a malformed packet.
CVE-2012-4292	The dissect_stun_message function in epan/dissectors/packet-stun.c in the STUN dissector in Wireshark 1.4.x before 1.4.15, 1.6.x before 1.6.10, and 1.8.x before 1.8.2 does not properly interact with key-destruction behavior in a certain tree library, which allows remote attackers to cause a denial of service (application crash) via a malformed packet.
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-2012-4398	The __request_module function in kernel/kmod.c in the Linux kernel before 3.4 does not set a certain killable attribute, which allows local users to cause a denial of service (memory consumption) via a crafted application.
CVE-2012-4405	Multiple integer underflows in the icmLut_allocate function in International Color Consortium (ICC) Format library (icclib), as used in Ghostscript 9.06 and Argyll Color Management System, allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted (1) PostScript or (2) PDF file with embedded images, which triggers a heap-based buffer overflow. NOTE: this issue is also described as an array index error.
CVE-2012-4416	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, and 6 Update 35 and earlier, allows remote attackers to affect confidentiality and integrity via unknown vectors related to Hotspot.
CVE-2012-4444	The ip6_frag_queue function in net/ipv6/reassembly.c in the Linux kernel before 2.6.36 allows remote attackers to bypass intended network restrictions via overlapping IPv6 fragments.
CVE-2012-4447	Heap-based buffer overflow in tif_pixarlog.c in LibTIFF before 4.0.3 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted TIFF image using the PixarLog Compression format.
CVE-2012-4453	dracut.sh in dracut, as used in Red Hat Enterprise Linux 6, Fedora 16 and 17, and possibly other products, creates initramfs images with world-readable permissions, which might allow local users to obtain sensitive information.
CVE-2012-4461	The KVM subsystem in the Linux kernel before 3.6.9, when running on hosts that use qemu userspace without XSAVE, allows local users to cause a denial of service (kernel OOPS) by using the KVM_SET_SREGS ioctl to set the X86_CR4_OSXSAVE bit in the guest cr4 register, then calling the KVM_RUN ioctl.
CVE-2012-4466	Ruby 1.8.7 before patchlevel 371, 1.9.3 before patchlevel 286, and 2.0 before revision r37068 allows context-dependent attackers to bypass safe-level restrictions and modify untainted strings via the name_err_mesg_to_str API function, which marks the string as tainted, a different vulnerability than CVE-2011-1005.
CVE-2012-4481	The safe-level feature in Ruby 1.8.7 allows context-dependent attackers to modify strings via the NameError#to_s method when operating on Ruby

	objects. NOTE: this issue is due to an incomplete fix for CVE-2011-1005.
CVE-2012-4505	Heap-based buffer overflow in the px_pac_reload function in lib/pac.c in libproxy 0.2.x and 0.3.x allows remote servers to have an unspecified impact via a crafted Content-Length size in an HTTP response header for a proxy.pac file request, a different vulnerability than CVE-2012-4504.
CVE-2012-4508	Race condition in fs/ext4/extents.c in the Linux kernel before 3.4.16 allows local users to obtain sensitive information from a deleted file by reading an extent that was not properly marked as uninitialized.
CVE-2012-4516	librdmacm 1.0.16, when ibacm.port is not specified, connects to port 6125, which allows remote attackers to specify the address resolution information for the application via a malicious ib_acm service.
CVE-2012-4530	The load_script function in fs/binfmt_script.c in the Linux kernel before 3.7.2 does not properly handle recursion, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.
CVE-2012-4558	Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manager interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.
CVE-2012-4564	ppm2tiff does not check the return value of the TIFFScanlineSize function, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted PPM image that triggers an integer overflow, a zero-memory allocation, and a heap-based buffer overflow.
CVE-2012-4565	The tcp_illinois_info function in net/ipv4/tcp_illinois.c in the Linux kernel before 3.4.19, when the net.ipv4.tcp_congestion_control illinois setting is enabled, allows local users to cause a denial of service (divide-by-zero error and OOPS) by reading TCP stats.
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-2012-4929	The TLS protocol 1.2 and earlier, as used in Mozilla Firefox, Google Chrome, Qt, and other products, can encrypt compressed data without properly obfuscating the length of the unencrypted data, which allows man-in-the-middle attackers to obtain plaintext HTTP headers by observing length differences during a series of guesses in which a string in an HTTP request potentially matches an unknown string in an HTTP header, aka a "CRIME" attack.
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-2012-5068	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7

	Update 7 and earlier, and 6 Update 35 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.
CVE-2012-5075	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, 6 Update 35 and earlier, and 5.0 Update 36 and earlier allows remote attackers to affect confidentiality, related to JMX.
CVE-2012-5077	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, 6 Update 35 and earlier, 5.0 Update 36 and earlier, and 1.4.2_38 and earlier allows remote attackers to affect confidentiality via unknown vectors related to Security.
CVE-2012-5079	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, 6 Update 35 and earlier, 5.0 Update 36 and earlier, and 1.4.2_38 and earlier allows remote attackers to affect integrity via unknown vectors related to Libraries, a different vulnerability than CVE-2012-5073.
CVE-2012-5081	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, 6 Update 35 and earlier, 5.0 Update 36 and earlier, and 1.4.2_38 and earlier allows remote attackers to affect availability, related to JSSE.
CVE-2012-5085	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, 6 Update 35 and earlier, 5.0 Update 36 and earlier, and 1.4.2_38 and earlier allows remote authenticated users to have an unspecified impact via unknown vectors related to Networking. NOTE: the Oracle CPU states that this issue has a 0.0 CVSS score. If so, then this is not a vulnerability and this issue should not be included in CVE.
CVE-2012-5086	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 7 and earlier, and 6 Update 35 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Beans.
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-2012-5166	ISC BIND 9.x before 9.7.6-P4, 9.8.x before 9.8.3-P4, 9.9.x before 9.9.1-P4, and 9.4-ESV and 9.6-ESV before 9.6-ESV-R7-P4 allows remote attackers to cause a denial of service (named daemon hang) via unspecified combinations of resource records.
CVE-2012-5195	Heap-based buffer overflow in the Perl_repeatcpy function in util.c in Perl 5.12.x before 5.12.5, 5.14.x before 5.14.3, and 5.15.x before 15.15.5 allows context-dependent attackers to cause a denial of service (memory consumption and crash) or possibly execute arbitrary code via the 'x' string repeat operator.
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-2012-5517	The online_pages function in mm/memory_hotplug.c in the Linux kernel before 3.6 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact in opportunistic circumstances by using memory that was hot-added by an administrator.
CVE-2012-5519	CUPS 1.4.4, when running in certain Linux distributions such as Debian GNU/Linux, stores the web interface administrator key in /var/run/cups/certs/0 using certain permissions, which allows local users in the lpadmin group to read or write arbitrary files as root by leveraging the web interface.
CVE-2012-5526	CGI.pm module before 3.63 for Perl does not properly escape newlines in (1) Set-Cookie or (2) P3P headers, which might allow remote attackers to inject arbitrary headers into responses from applications that use CGI.pm.
CVE-2012-5533	The http_request_split_value function in request.c in lighttpd before 1.4.32 allows remote attackers to cause a denial of service (infinite loop) via a request with a

	header containing an empty token, as demonstrated using the "Connection: TE,,Keep-Alive" header.
CVE-2012-5536	A certain Red Hat build of the pam_ssh_agent_auth module on Red Hat Enterprise Linux (RHEL) 6 and Fedora Rawhide calls the glibc error function instead of the error function in the OpenSSH codebase, which allows local users to obtain sensitive information from process memory or possibly gain privileges via crafted use of an application that relies on this module, as demonstrated by su and sudo.
CVE-2012-5581	Stack-based buffer overflow in tif_dir.c in LibTIFF before 4.0.2 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted DOTRANGE tag in a TIFF image.
CVE-2012-5611	Stack-based buffer overflow in the acl_get function in Oracle MySQL 5.5.19 and other versions through 5.5.28, and 5.1.53 and other versions through 5.1.66, and MariaDB 5.5.2.x before 5.5.28a, 5.3.x before 5.3.11, 5.2.x before 5.2.13 and 5.1.x before 5.1.66, allows remote authenticated users to execute arbitrary code via a long argument to the GRANT FILE command.
CVE-2012-5614	Oracle MySQL 5.1.67 and earlier and 5.5.29 and earlier, and MariaDB 5.5.28a and possibly other versions, allows remote authenticated users to cause a denial of service (mysqld crash) via a SELECT command with an UpdateXML command containing XML with a large number of unique, nested elements.
CVE-2012-5657	The (1) Zend_Feed_Rss and (2) Zend_Feed_Atom classes in Zend_Feed in Zend Framework 1.11.x before 1.11.15 and 1.12.x before 1.12.1 allow remote attackers to read arbitrary files, send HTTP requests to intranet servers, and possibly cause a denial of service (CPU and memory consumption) via an XML External Entity (XXE) attack.
CVE-2012-5667	Multiple integer overflows in GNU Grep before 2.11 might allow context-dependent attackers to execute arbitrary code via vectors involving a long input line that triggers a heap-based buffer overflow.
CVE-2012-5669	The _bdf_parse_glyphs function in FreeType before 2.4.11 allows context-dependent attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to BDF fonts and an incorrect calculation that triggers an out-of-bounds read.
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-2012-5688	ISC BIND 9.8.x before 9.8.4-P1 and 9.9.x before 9.9.2-P1, when DNS64 is enabled, allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.
CVE-2012-5689	ISC BIND 9.8.x through 9.8.4-P1 and 9.9.x through 9.9.2-P1, in certain configurations involving DNS64 with a Response Policy Zone that lacks an AAAA rewrite rule, allows remote attackers to cause a denial of service (assertion failure and named daemon exit) via a query for an AAAA record.
CVE-2012-5783	Apache Commons HttpClient 3.x, as used in Amazon Flexible Payments Service (FPS) merchant Java SDK and other products, does not verify that the server

	hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.
CVE-2012-5784	Apache Axis 1.4 and earlier, as used in PayPal Payments Pro, PayPal Mass Pay, PayPal Transactional Information SOAP, the Java Message Service implementation in Apache ActiveMQ, and other products, does not verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.
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-2012-6056	Integer overflow in the dissect_sack_chunk function in epan/dissectors/packet-sctp.c in the SCTP dissector in Wireshark 1.8.x before 1.8.4 allows remote attackers to cause a denial of service (infinite loop) via a crafted Duplicate TSN count.
CVE-2012-6059	The dissect_isakmp function in epan/dissectors/packet-isakmp.c in the ISAKMP dissector in Wireshark 1.6.x before 1.6.12 and 1.8.x before 1.8.4 uses an incorrect data structure to determine IKEv2 decryption parameters, which allows remote attackers to cause a denial of service (application crash) via a malformed packet.
CVE-2012-6060	Integer overflow in the dissect_iscsi_pdu function in epan/dissectors/packet-iscsi.c in the iSCSI dissector in Wireshark 1.6.x before 1.6.12 and 1.8.x before 1.8.4 allows remote attackers to cause a denial of service (infinite loop) via a malformed packet.
CVE-2012-6061	The dissect_wtp_common function in epan/dissectors/packet-wtp.c in the WTP dissector in Wireshark 1.6.x before 1.6.12 and 1.8.x before 1.8.4 uses an incorrect data type for a certain length field, which allows remote attackers to cause a denial of service (integer overflow and infinite loop) via a crafted value in a packet.

CVE-2012-6062	The dissect_rtcp_app function in epan/dissectors/packet-rtcp.c in the RTCP dissector in Wireshark 1.6.x before 1.6.12 and 1.8.x before 1.8.4 allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.
CVE-2012-6151	Net-SNMP 5.7.1 and earlier, when AgentX is registering to handle a MIB and processing GETNEXT requests, allows remote attackers to cause a denial of service (crash or infinite loop, CPU consumption, and hang) by causing the AgentX subagent to timeout.
CVE-2012-6153	http/conn/ssl/AbstractVerifier.java in Apache Commons HttpClient before 4.2.3 does not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via a certificate with a subject that specifies a common name in a field that is not the CN field. NOTE: this issue exists because of an incomplete fix for CVE-2012-5783.
CVE-2012-6329	The _compile function in Maketext.pm in the Locale::Maketext implementation in Perl before 5.17.7 does not properly handle backslashes and fully qualified method names during compilation of bracket notation, which allows context-dependent attackers to execute arbitrary commands via crafted input to an application that accepts translation strings from users, as demonstrated by the TWiki application before 5.1.3, and the Foswiki application 1.0.x through 1.0.10 and 1.1.x through 1.1.6.
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-2012-6544	The Bluetooth protocol stack in the Linux kernel before 3.6 does not properly initialize certain structures, which allows local users to obtain sensitive information from kernel stack memory via a crafted application that targets the (1) L2CAP or (2) HCI implementation.
CVE-2012-6545	The Bluetooth RFCOMM implementation in the Linux kernel before 3.6 does not properly initialize certain structures, which allows local users to obtain sensitive information from kernel memory via a crafted application.
CVE-2012-6548	The udf_encode_fh function in fs/udf/namei.c in the Linux kernel before 3.6 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel heap memory via a crafted application.

CVE-2013-0166	OpenSSL before 0.9.8y, 1.0.0 before 1.0.0k, and 1.0.1 before 1.0.1d does not properly perform signature verification for OCSP responses, which allows remote OCSP servers to cause a denial of service (NULL pointer dereference and application crash) via an invalid key.
CVE-2013-0169	The TLS protocol 1.1 and 1.2 and the DTLS protocol 1.0 and 1.2, as used in OpenSSL, OpenJDK, PolarSSL, and other products, do not properly consider timing side-channel attacks on a MAC check requirement 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, aka the "Lucky Thirteen" issue.
CVE-2013-0190	The xen_failsafe_callback function in Xen for the Linux kernel 2.6.23 and other versions, when running a 32-bit PVOPS guest, allows local users to cause a denial of service (guest crash) by triggering an iret fault, leading to use of an incorrect stack pointer and stack corruption.
CVE-2013-0221	The SUSE coreutils-i18n.patch for GNU coreutils allows context-dependent attackers to cause a denial of service (segmentation fault and crash) via a long string to the sort command, when using the (1) -d or (2) -M switch, which triggers a stack-based buffer overflow in the alloca function.
CVE-2013-0222	The SUSE coreutils-i18n.patch for GNU coreutils allows context-dependent attackers to cause a denial of service (segmentation fault and crash) via a long string to the uniq command, which triggers a stack-based buffer overflow in the alloca function.
CVE-2013-0223	The SUSE coreutils-i18n.patch for GNU coreutils allows context-dependent attackers to cause a denial of service (segmentation fault and crash) via a long string to the join command, when using the -i switch, which triggers a stack-based buffer overflow in the alloca function.
CVE-2013-0242	Buffer overflow in the extend_buffers function in the regular expression matcher (posix/regexec.c) in glibc, possibly 2.17 and earlier, allows context-dependent attackers to cause a denial of service (memory corruption and crash) via crafted multibyte characters.
CVE-2013-0255	PostgreSQL 9.2.x before 9.2.3, 9.1.x before 9.1.8, 9.0.x before 9.0.12, 8.4.x before 8.4.16, and 8.3.x before 8.3.23 does not properly declare the enum_recv function in backend/utils/adt/enum.c, which causes it to be invoked with incorrect arguments and allows remote authenticated users to cause a denial of service (server crash) or read sensitive process memory via a crafted

	SQL command, which triggers an array index error and an out-of-bounds read.
CVE-2013-0338	libxml2 2.9.0 and earlier allows context-dependent attackers to cause a denial of service (CPU and memory consumption) via an XML file containing an entity declaration with long replacement text and many references to this entity, aka "internal entity expansion" with linear complexity.
CVE-2013-0343	The ipv6_create_tempaddr function in net/ipv6/addrconf.c in the Linux kernel through 3.8 does not properly handle problems with the generation of IPv6 temporary addresses, which allows remote attackers to cause a denial of service (excessive retries and address-generation outage), and consequently obtain sensitive information, via ICMPv6 Router Advertisement (RA) messages.
CVE-2013-0345	varnish 3.0.3 uses world-readable permissions for the /var/log/varnish/ directory and the log files in the directory, which allows local users to obtain sensitive information by reading the files. NOTE: some of these details are obtained from third party information.
CVE-2013-0401	The Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, 6 Update 43 and earlier, and 5.0 Update 41 and earlier; and OpenJDK 6 and 7; allows remote attackers to execute arbitrary code via vectors related to AWT, as demonstrated by Ben Murphy during a Pwn2Own competition at CanSecWest 2013. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to invocation of the system class loader by the sun.awt.datatransfer.ClassLoaderObjectInputStream class, which allows remote attackers to bypass Java sandbox restrictions.
CVE-2013-0424	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, 5.0 through Update 38, and 1.4.2_40 and earlier, and OpenJDK 7, allows remote attackers to affect integrity via vectors related to RMI. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to cross-site scripting (XSS) in the sun.rmi.transport.proxy CGIHandler class that does not properly handle error messages in a (1) command or (2) port number.
CVE-2013-0425	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, 5.0 through Update 38, and 1.4.2_40 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality,

	integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2013-0428 and CVE-2013-0426. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to incorrect "access control checks" in the logging API that allow remote attackers to bypass Java sandbox restrictions.
CVE-2013-0426	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, 5.0 through Update 38, and 1.4.2_40 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2013-0425 and CVE-2013-0428. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to incorrect "access control checks" in the logging API that allow remote attackers to bypass Java sandbox restrictions.
CVE-2013-0427	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, and 5.0 through Update 38, and OpenJDK 6 and 7, allows remote attackers to affect integrity via unknown vectors related to Libraries. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to interrupt certain threads that should not be interrupted.
CVE-2013-0428	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, 5.0 through Update 38, and 1.4.2_40 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2013-0425 and CVE-2013-0426. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "incorrect checks for proxy classes" in the Reflection API.
CVE-2013-0429	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, and 5.0 through Update 38, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to CORBA. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue involves the creation of a single

	PresentationManager that is shared across multiple thread groups, which allows remote attackers to bypass Java sandbox restrictions.
CVE-2013-0431	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, and OpenJDK 7, allows user-assisted remote attackers to bypass the Java security sandbox via unspecified vectors related to JMX, aka "Issue 52," a different vulnerability than CVE-2013-1490.
CVE-2013-0432	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, 5.0 through Update 38, and 1.4.2_40 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality and integrity via vectors related to AWT. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "insufficient clipboard access premission checks."
CVE-2013-0433	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, and 5.0 through Update 38, and OpenJDK 6 and 7, allows remote attackers to affect integrity via unknown vectors related to Networking. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to avoid triggering an exception during the deserialization of invalid InetSocketAddress data.
CVE-2013-0434	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, 5.0 through Update 38, and 1.4.2_40 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality via vectors related to JAXP. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to the public declaration of the loadPropertyFile method in the JAXP FuncSystemProperty class, which allows remote attackers to obtain sensitive information.
CVE-2013-0435	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11 and 6 through Update 38, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality via vectors related to JAX-WS. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to improper

	restriction of com.sun.xml.internal packages and "Better handling of UI elements."
CVE-2013-0440	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, 5.0 through Update 38, and 1.4.2_40 and earlier, and OpenJDK 7, allows remote attackers to affect availability via vectors related to JSSE. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to CPU consumption in the SSL/TLS implementation via a large number of ClientHello packets that are not properly handled by (1) ClientHandshaker.java and (2) ServerHandshaker.java.
CVE-2013-0441	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, 5.0 through Update 38, and 1.4.2_40 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to CORBA, a different vulnerability than CVE-2013-1476 and CVE-2013-1475. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to bypass Java sandbox restrictions via certain methods that should not be serialized, aka "missing serialization restriction."
CVE-2013-0442	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, 5.0 through Update 38, and 1.4.2_40 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to AWT. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to an improper check of "privileges of the code" that bypasses the sandbox.
CVE-2013-0443	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, 5.0 through Update 38, and 1.4.2_40 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality and integrity via vectors related to JSSE. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to incorrect validation of Diffie-Hellman keys, which allows remote attackers to conduct a "small subgroup attack" to force the use of weak session keys or obtain sensitive information about the private key.

CVE-2013-0444	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, and OpenJDK 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Beans. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "insufficient checks for cached results" by the Java Beans MethodFinder, which might allow attackers to access methods that should only be accessible to privileged code.
CVE-2013-0445	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, and 5.0 through Update 38, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to AWT. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to an improper check of "privileges of the code" that bypasses the sandbox.
CVE-2013-0450	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, and 5.0 through Update 38, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JMX. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to improper checks of "access control context" in the JMX RequiredModelMBean class.
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-2013-0791	The CERT_DecodeCertPackage function in Mozilla Network Security Services (NSS), as used in Mozilla Firefox before 20.0, Firefox ESR 17.x before 17.0.5, Thunderbird before 17.0.5, Thunderbird ESR 17.x before 17.0.5, SeaMonkey before 2.17, and other products, allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) via a crafted certificate.
CVE-2013-0809	Unspecified vulnerability in the 2D component in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 15 and earlier, 6 Update 41 and earlier, and 5.0 Update 40 and earlier allows remote attackers to execute arbitrary code via unknown vectors, a different vulnerability than CVE-2013-1493.
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-2013-0871	Race condition in the ptrace functionality in the Linux kernel before 3.7.5 allows local users to gain privileges via a PTRACE_SETREGS ptrace system call in a crafted application, as demonstrated by ptrace_death.
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-2013-0914	The flush_signal_handlers function in kernel/signal.c in the Linux kernel before 3.8.4 preserves the value of the sa_restorer field across an exec operation, which makes it easier for local users to bypass the ASLR protection mechanism via a crafted application containing a sigaction system call.
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-2013-1059	net/ceph/auth_none.c in the Linux kernel through 3.10 allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via an auth_reply message that triggers an attempted build_request operation.
CVE-2013-1362	Incomplete blacklist vulnerability in nrpc.c in Nagios Remote Plug-In Executor (NRPE) before 2.14 might allow remote attackers to execute arbitrary shell commands via "$()" shell metacharacters, which are processed by bash.
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-2013-1416	The prep_reprocess_req function in do_tgs_req.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.10.5 does not properly perform service-principal realm referral, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted TGS-REQ request.
CVE-2013-1418	The setup_server_realm function in main.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.10.7, when multiple realms are configured, allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted request.
CVE-2013-1434	Multiple SQL injection vulnerabilities in (1) api_poller.php and (2) utility.php in Cacti before 0.8.8b

	allow remote attackers to execute arbitrary SQL commands via unspecified vectors.
CVE-2013-1435	(1) snmp.php and (2) rrd.php in Cacti before 0.8.8b allows remote attackers to execute arbitrary commands via shell metacharacters in unspecified vectors.
CVE-2013-1445	The Crypto.Random.atfork function in PyCrypto before 2.6.1 does not properly reseed the pseudo-random number generator (PRNG) before allowing a child process to access it, which makes it easier for context-dependent attackers to obtain sensitive information by leveraging a race condition in which a child process is created and accesses the PRNG within the same rate-limit period as another process.
CVE-2013-1447	OpenJPEG 1.3 and earlier allows remote attackers to cause a denial of service (memory consumption or crash) via unspecified vectors related to NULL pointer dereferences, division-by-zero, and other errors.
CVE-2013-1475	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, 5.0 through Update 38, and 1.4.2_40 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to CORBA. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "IIOP type reuse management" in ObjectStreamClass.java.
CVE-2013-1476	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, 5.0 through Update 38, and 1.4.2_40 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to CORBA, a different vulnerability than CVE-2013-0441 and CVE-2013-1475. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to bypass Java sandbox restrictions via "certain value handler constructors."
CVE-2013-1478	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, 5.0 through Update 38, and 1.4.2_40 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "insufficient validation of raster parameters" that can trigger an integer overflow and memory corruption.

CVE-2013-1480	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 through Update 11, 6 through Update 38, 5.0 through Update 38, and 1.4.2_40 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to AWT. NOTE: the previous information is from the February 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "insufficient validation of raster parameters" in awt_parseImage.c, which triggers memory corruption.
CVE-2013-1484	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 13 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.
CVE-2013-1485	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 13 and earlier allows remote attackers to affect integrity via unknown vectors related to Libraries.
CVE-2013-1486	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 13 and earlier, 6 Update 39 and earlier, and 5.0 Update 39 and earlier allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JMX.
CVE-2013-1488	The Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, and OpenJDK 6 and 7, allows remote attackers to execute arbitrary code via unspecified vectors involving reflection, Libraries, "improper toString calls," and the JDBC driver manager, as demonstrated by James Forshaw during a Pwn2Own competition at CanSecWest 2013.
CVE-2013-1493	The color management (CMM) functionality in the 2D component in Oracle Java SE 7 Update 15 and earlier, 6 Update 41 and earlier, and 5.0 Update 40 and earlier allows remote attackers to execute arbitrary code or cause a denial of service (crash) via an image with crafted raster parameters, which triggers (1) an out-of-bounds read or (2) memory corruption in the JVM, as exploited in the wild in February 2013.
CVE-2013-1500	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows local users to affect confidentiality and integrity via unknown vectors related to 2D. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to weak permissions for shared memory.

CVE-2013-1506	Unspecified vulnerability in Oracle MySQL 5.1.67 and earlier, 5.5.29 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Locking.
CVE-2013-1518	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, 6 Update 43 and earlier, and 5.0 Update 41 and earlier; and OpenJDK 6 and 7; allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JAXP. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "missing security restrictions."
CVE-2013-1521	Unspecified vulnerability in Oracle MySQL 5.1.67 and earlier and 5.5.29 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Server Locking.
CVE-2013-1531	Unspecified vulnerability in Oracle MySQL 5.1.66 and earlier and 5.5.28 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Server Privileges.
CVE-2013-1532	Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Information Schema.
CVE-2013-1537	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, 6 Update 43 and earlier, and 5.0 Update 41 and earlier; and OpenJDK 6 and 7; allows remote attackers to affect confidentiality, integrity, and availability via vectors related to RMI. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to the default java.rmi.server.useCodebaseOnly setting of false, which allows remote attackers to perform "dynamic class downloading" and execute arbitrary code.
CVE-2013-1544	Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Data Manipulation Language.
CVE-2013-1548	Unspecified vulnerability in Oracle MySQL 5.1.63 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Types.
CVE-2013-1552	Unspecified vulnerability in Oracle MySQL 5.1.67 and earlier and 5.5.29 and earlier allows remote

	authenticated users to affect confidentiality, integrity, and availability via unknown vectors.
CVE-2013-1555	Unspecified vulnerability in Oracle MySQL 5.1.67 and earlier, and 5.5.29 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server Partition.
CVE-2013-1557	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, 6 Update 43 and earlier, and 5.0 Update 41 and earlier; and OpenJDK 6 and 7; allows remote attackers to affect confidentiality, integrity, and availability via vectors related to RMI. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "missing security restrictions" in the LogStream.setDefaultStream method.
CVE-2013-1558	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier and 6 Update 43 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Beans.
CVE-2013-1569	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, 6 Update 43 and earlier, and 5.0 Update 41 and earlier; and OpenJDK 6 and 7; allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "checking of [a] glyph table" in the International Components for Unicode (ICU) Layout Engine before 51.2.
CVE-2013-1571	Unspecified vulnerability in the Javadoc component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier; JavaFX 2.2.21 and earlier; and OpenJDK 7 allows remote attackers to affect integrity via unknown vectors related to Javadoc. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to frame injection in HTML that is generated by Javadoc.
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-2013-1619	The TLS implementation in GnuTLS before 2.12.23, 3.0.x before 3.0.28, and 3.1.x before 3.1.7 does not properly consider timing side-channel attacks on a noncompliant 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-2013-1620	The TLS implementation in Mozilla Network Security Services (NSS) does not properly consider timing side-channel attacks on a noncompliant 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-2013-1640	The (1) template and (2) inline_template functions in the master server in Puppet before 2.6.18, 2.7.x before 2.7.21, and 3.1.x before 3.1.1, and Puppet Enterprise before 1.2.7 and 2.7.x before 2.7.2 allows remote authenticated users to execute arbitrary code via a crafted catalog request.
CVE-2013-1667	The rehash mechanism in Perl 5.8.2 through 5.16.x allows context-dependent attackers to cause a denial of service (memory consumption and crash) via a crafted hash key.
CVE-2013-1739	Mozilla Network Security Services (NSS) before 3.15.2 does not ensure that data structures are initialized before read operations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a decryption failure.
CVE-2013-1741	Integer overflow in Mozilla Network Security Services (NSS) 3.15 before 3.15.3 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large size value.
CVE-2013-1752	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the

	candidate has been publicized, the details for this candidate will beprovided.
CVE-2013-1753	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2013-1767	Use-after-free vulnerability in the shmem_remount_fs function in mm/shmem.c in the Linux kernel before 3.7.10 allows local users to gain privileges or cause a denial of service (system crash) by remounting a tmpfs filesystem without specifying a required mpol (aka mempolicy) mount option.
CVE-2013-1773	Buffer overflow in the VFAT filesystem implementation in the Linux kernel before 3.3 allows local users to gain privileges or cause a denial of service (system crash) via a VFAT write operation on a filesystem with the utf8 mount option, which is not properly handled during UTF-8 to UTF-16 conversion.
CVE-2013-1775	sudo 1.6.0 through 1.7.10p6 and sudo 1.8.0 through 1.8.6p6 allows local users or physically proximate attackers to bypass intended time restrictions and retain privileges without re-authenticating by setting the system clock and sudo user timestamp to the epoch.
CVE-2013-1821	lib/rexml/text.rb in the REXML parser in Ruby before 1.9.3-p392 allows remote attackers to cause a denial of service (memory consumption and crash) via crafted text nodes in an XML document, aka an XML Entity Expansion (XEE) attack.
CVE-2013-1845	The mod_dav_svn Apache HTTPD server module in Subversion 1.6.x before 1.6.21 and 1.7.0 through 1.7.8 allows remote authenticated users to cause a denial of service (memory consumption) by (1) setting or (2) deleting a large number of properties for a file or directory.
CVE-2013-1846	The mod_dav_svn Apache HTTPD server module in Subversion 1.6.x before 1.6.21 and 1.7.0 through 1.7.8 allows remote authenticated users to cause a denial of service (NULL pointer dereference and crash) via a LOCK on an activity URL.
CVE-2013-1847	The mod_dav_svn Apache HTTPD server module in Subversion 1.6.0 through 1.6.20 and 1.7.0 through 1.7.8 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via an anonymous LOCK for a URL that does not exist.
CVE-2013-1848	fs/ext3/super.c in the Linux kernel before 3.8.4 uses incorrect arguments to functions in certain circumstances related to printk input, which allows local

	users to conduct format-string attacks and possibly gain privileges via a crafted application.
CVE-2013-1849	The mod_dav_svn Apache HTTPD server module in Subversion 1.6.x through 1.6.20 and 1.7.0 through 1.7.8 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a PROPFIND request for an activity URL.
CVE-2013-1862	mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary commands via an HTTP request containing an escape sequence for a terminal emulator.
CVE-2013-1872	The Intel drivers in Mesa 8.0.x and 9.0.x allow context-dependent attackers to cause a denial of service (reachable assertion and crash) and possibly execute arbitrary code via vectors involving 3d graphics that trigger an out-of-bounds array access, related to the fs_visitor::remove_dead_constants function. NOTE: this issue might be related to CVE-2013-0796.
CVE-2013-1897	The do_search function in ldap/servers/slapd/search.c in 389 Directory Server 1.2.x before 1.2.11.20 and 1.3.x before 1.3.0.5 does not properly restrict access to entries when the nsslapd-allow-anonymous-access configuration is set to rootdse and the BASE search scope is used, which allows remote attackers to obtain sensitive information outside of the rootDSE via a crafted LDAP search.
CVE-2013-1899	Argument injection vulnerability in PostgreSQL 9.2.x before 9.2.4, 9.1.x before 9.1.9, and 9.0.x before 9.0.13 allows remote attackers to cause a denial of service (file corruption), and allows remote authenticated users to modify configuration settings and execute arbitrary code, via a connection request using a database name that begins with a "-" (hyphen).
CVE-2013-1900	PostgreSQL 9.2.x before 9.2.4, 9.1.x before 9.1.9, 9.0.x before 9.0.13, and 8.4.x before 8.4.17, when using OpenSSL, generates insufficiently random numbers, which might allow remote authenticated users to have an unspecified impact via vectors related to the "contrib/pgcrypto functions."
CVE-2013-1901	PostgreSQL 9.2.x before 9.2.4 and 9.1.x before 9.1.9 does not properly check REPLICATION privileges, which allows remote authenticated users to bypass intended backup restrictions by calling the (1) pg_start_backup or (2) pg_stop_backup functions.
CVE-2013-1914	Stack-based buffer overflow in the getaddrinfo function in sysdeps/posix/getaddrinfo.c in GNU C Library (aka glibc or libc6) 2.17 and earlier allows remote attackers to cause a denial of service (crash) via a (1) hostname

	or (2) IP address that triggers a large number of domain conversion results.
CVE-2013-1929	Heap-based buffer overflow in the tg3_read_vpd function in drivers/net/ethernet/broadcom/tg3.c in the Linux kernel before 3.8.6 allows physically proximate attackers to cause a denial of service (system crash) or possibly execute arbitrary code via crafted firmware that specifies a long string in the Vital Product Data (VPD) data structure.
CVE-2013-1940	X.Org X server before 1.13.4 and 1.4.x before 1.14.1 does not properly restrict access to input events when adding a new hot-plug device, which might allow physically proximate attackers to obtain sensitive information, as demonstrated by reading passwords from a tty.
CVE-2013-1944	The tailMatch function in cookie.c in cURL and libcurl before 7.30.0 does not properly match the path domain when sending cookies, which allows remote attackers to steal cookies via a matching suffix in the domain of a URL.
CVE-2013-1950	The svc_dg_getargs function in libtirpc 0.2.3 and earlier allows remote attackers to cause a denial of service (rpcbind crash) via a Sun RPC request with crafted arguments that trigger a free of an invalid pointer.
CVE-2013-1960	Heap-based buffer overflow in the t2p_process_jpeg_strip function in tiff2pdf in libtiff 4.0.3 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted TIFF image file.
CVE-2013-1961	Stack-based buffer overflow in the t2p_write_pdf_page function in tiff2pdf in libtiff before 4.0.3 allows remote attackers to cause a denial of service (application crash) via a crafted image length and resolution in a TIFF image file.
CVE-2013-1976	The (1) tomcat5, (2) tomcat6, and (3) tomcat7 init scripts, as used in the RPM distribution of Tomcat for JBoss Enterprise Web Server 1.0.2 and 2.0.0, and Red Hat Enterprise Linux 5 and 6, allow local users to change the ownership of arbitrary files via a symlink attack on (a) tomcat5-initd.log, (b) tomcat6-initd.log, (c) catalina.out, or (d) tomcat7-initd.log.
CVE-2013-1981	Multiple integer overflows in X.org libX11 1.5.99.901 (1.6 RC1) and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XQueryFont, (2) _XF86BigfontQueryFont, (3) XListFontsWithInfo, (4) XGetMotionEvents, (5) XListHosts, (6) XGetModifierMapping, (7) XGetPointerMapping, (8) XGetKeyboardMapping, (9) XGetWindowProperty, (10) XGetImage, (11) LoadColornameDB, (12)

	XrmGetFileDatabase, (13) _XimParseStringFile, or (14) TransFileName functions.
CVE-2013-1982	Multiple integer overflows in X.org libXext 1.3.1 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XcupGetReservedColormapEntries, (2) XcupStoreColors, (3) XdbeGetVisualInfo, (4) XeviGetVisualInfo, (5) XShapeGetRectangles, and (6) XSyncListSystemCounters functions.
CVE-2013-1983	Integer overflow in X.org libXfixes 5.0 and earlier allows X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the XFixesGetCursorImage function.
CVE-2013-1984	Multiple integer overflows in X.org libXi 1.7.1 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XGetDeviceControl, (2) XGetFeedbackControl, (3) XGetDeviceDontPropagateList, (4) XGetDeviceMotionEvents, (5) XIGetProperty, (6) XIGetSelectedEvents, (7) XGetDeviceProperties, and (8) XListInputDevices functions.
CVE-2013-1985	Integer overflow in X.org libXinerama 1.1.2 and earlier allows X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the XineramaQueryScreens function.
CVE-2013-1986	Multiple integer overflows in X.org libXrandr 1.4.0 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XRRQueryOutputProperty and (2) XRRQueryProviderProperty functions.
CVE-2013-1987	Multiple integer overflows in X.org libXrender 0.9.7 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XRenderQueryFilters, (2) XRenderQueryFormats, and (3) XRenderQueryPictIndexValues functions.
CVE-2013-1988	Multiple integer overflows in X.org libXRes 1.0.6 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XResQueryClients and (2) XResQueryClientResources functions.
CVE-2013-1989	Multiple integer overflows in X.org libXv 1.0.7 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XvQueryPortAttributes, (2) XvListImageFormats, and (3) XvCreateImage function.
CVE-2013-1990	Multiple integer overflows in X.org libXvMC 1.0.7 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XvMCListSurfaceTypes and (2) XvMCListSubpictureTypes functions.

CVE-2013-1991	Multiple integer overflows in X.org libXxf86dga 1.1.3 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XDGAQueryModes and (2) XDGASetMode functions.
CVE-2013-1993	Multiple integer overflows in X.org libGLX in Mesa 9.1.1 and earlier allow X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the (1) XF86DRIOpenConnection and (2) XF86DRIGetClientDriverName functions.
CVE-2013-1995	X.org libXi 1.7.1 and earlier allows X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to an unexpected sign extension in the XListInputDevices function.
CVE-2013-1997	Multiple buffer overflows in X.org libX11 1.5.99.901 (1.6 RC1) and earlier allow X servers to cause a denial of service (crash) and possibly execute arbitrary code via crafted length or index values to the (1) XAllocColorCells, (2) _XkbReadGetDeviceInfoReply, (3) _XkbReadGeomShapes, (4) _XkbReadGetGeometryReply, (5) _XkbReadKeySyms, (6) _XkbReadKeyActions, (7) _XkbReadKeyBehaviors, (8) _XkbReadModifierMap, (9) _XkbReadExplicitComponents, (10) _XkbReadVirtualModMap, (11) _XkbReadGetNamesReply, (12) _XkbReadGetMapReply, (13) _XimXGetReadData, (14) XListFonts, (15) XListExtensions, and (16) XGetFontPath functions.
CVE-2013-1998	Multiple buffer overflows in X.org libXi 1.7.1 and earlier allow X servers to cause a denial of service (crash) and possibly execute arbitrary code via crafted length or index values to the (1) XGetDeviceButtonMapping, (2) XIPassiveGrabDevice, and (3) XQueryDeviceState functions.
CVE-2013-1999	Buffer overflow in X.org libXvMC 1.0.7 and earlier allows X servers to cause a denial of service (crash) and possibly execute arbitrary code via crafted length or index values to the XvMCGetDRInfo function.
CVE-2013-2000	Multiple buffer overflows in X.org libXxf86dga 1.1.3 and earlier allow X servers to cause a denial of service (crash) and possibly execute arbitrary code via crafted length or index values to the (1) XDGAQueryModes and (2) XDGASetMode functions.
CVE-2013-2001	Buffer overflow in X.org libXxf86vm 1.1.2 and earlier allows X servers to cause a denial of service (crash) and possibly execute arbitrary code via crafted length or index values to the XF86VidModeGetGammaRamp function.

CVE-2013-2002	Buffer overflow in X.org libXt 1.1.3 and earlier allows X servers to cause a denial of service (crash) and possibly execute arbitrary code via crafted length or index values to the _XtResourceConfigurationEH function.
CVE-2013-2003	Integer overflow in X.org libXcursor 1.1.13 and earlier allows X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the _XcursorFileHeaderCreate function.
CVE-2013-2004	The (1) GetDatabase and (2) _XimParseStringFile functions in X.org libX11 1.5.99.901 (1.6 RC1) and earlier do not restrict the recursion depth when processing directives to include files, which allows X servers to cause a denial of service (stack consumption) via a crafted file.
CVE-2013-2005	X.org libXt 1.1.3 and earlier does not check the return value of the XGetWindowProperty function, which allows X servers to trigger use of an uninitialized pointer and memory corruption via vectors related to the (1) ReqCleanup, (2) HandleSelectionEvents, (3) ReqTimedOut, (4) HandleNormal, and (5) HandleSelectionReplies functions.
CVE-2013-2028	The ngx_http_parse_chunked function in http/ngx_http_parse.c in nginx 1.3.9 through 1.4.0 allows remote attackers to cause a denial of service (crash) and execute arbitrary code via a chunked Transfer-Encoding request with a large chunk size, which triggers an integer signedness error and a stack-based buffer overflow.
CVE-2013-2029	nagios.upgrade_to_v3.sh, as distributed by Red Hat and possibly others for Nagios Core 3.4.4, 3.5.1, and earlier, allows local users to overwrite arbitrary files via a symlink attack on a temporary nagioscfg file with a predictable name in /tmp/.
CVE-2013-2053	Buffer overflow in the atodn function in Openswan before 2.6.39, when Opportunistic Encryption is enabled and an RSA key is being used, allows remote attackers to cause a denial of service (pluto IKE daemon crash) and possibly execute arbitrary code via crafted DNS TXT records. NOTE: this might be the same vulnerability as CVE-2013-2052 and CVE-2013-2054.
CVE-2013-2061	The openvpn_decrypt function in crypto.c in OpenVPN 2.3.0 and earlier, when running in UDP mode, allows remote attackers to obtain sensitive information via a timing attack involving an HMAC comparison function that does not run in constant time and a padding oracle attack on the CBC mode cipher.
CVE-2013-2062	Multiple integer overflows in X.org libXp 1.0.1 and earlier allow X servers to trigger allocation of insufficient

	memory and a buffer overflow via vectors related to the (1) XpGetAttributes, (2) XpGetOneAttribute, (3) XpGetPrinterList, and (4) XpQueryScreens functions.
CVE-2013-2063	Integer overflow in X.org libXtst 1.2.1 and earlier allows X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the XRecordGetContext function.
CVE-2013-2064	Integer overflow in X.org libxcb 1.9 and earlier allows X servers to trigger allocation of insufficient memory and a buffer overflow via vectors related to the read_packet function.
CVE-2013-2065	(1) DL and (2) Fiddle in Ruby 1.9 before 1.9.3 patchlevel 426, and 2.0 before 2.0.0 patchlevel 195, do not perform taint checking for native functions, which allows context-dependent attackers to bypass intended $SAFE level restrictions.
CVE-2013-2066	Buffer overflow in X.org libXv 1.0.7 and earlier allows X servers to cause a denial of service (crash) and possibly execute arbitrary code via crafted length or index values to the XvQueryPortAttributes function.
CVE-2013-2070	http/modules/ngx_http_proxy_module.c in nginx 1.1.4 through 1.2.8 and 1.3.0 through 1.4.0, when proxy_pass is used with untrusted HTTP servers, allows remote attackers to cause a denial of service (crash) and obtain sensitive information from worker process memory via a crafted proxy response, a similar vulnerability to CVE-2013-2028.
CVE-2013-2071	java/org/apache/catalina/core/AsyncContextImpl.java in Apache Tomcat 7.x before 7.0.40 does not properly handle the throwing of a RuntimeException in an AsyncListener in an application, which allows context-dependent attackers to obtain sensitive request information intended for other applications in opportunistic circumstances via an application that records the requests that it processes.
CVE-2013-2094	The perf_swevent_init function in kernel/events/core.c in the Linux kernel before 3.8.9 uses an incorrect integer data type, which allows local users to gain privileges via a crafted perf_event_open system call.
CVE-2013-2099	Algorithmic complexity vulnerability in the ssl.match_hostname function in Python 3.2.x, 3.3.x, and earlier, and unspecified versions of python-backports-ssl_match_hostname as used for older Python versions, allows remote attackers to cause a denial of service (CPU consumption) via multiple wildcard characters in the common name in a certificate.
CVE-2013-2110	Heap-based buffer overflow in the php_quot_print_encode function in ext/standard/quot_print.c in PHP before 5.3.26 and 5.4.x before 5.4.16 allows remote attackers to cause a denial

	of service (application crash) or possibly have unspecified other impact via a crafted argument to the quoted_printable_encode function.
CVE-2013-2116	The _gnutls_ciphertext2compressed function in lib/gnutls_cipher.c in GnuTLS 2.12.23 allows remote attackers to cause a denial of service (buffer over-read and crash) via a crafted padding length. NOTE: this might be due to an incorrect fix for CVE-2013-0169.
CVE-2013-2128	The tcp_read_sock function in net/ipv4/tcp.c in the Linux kernel before 2.6.34 does not properly manage skb consumption, which allows local users to cause a denial of service (system crash) via a crafted splice system call for a TCP socket.
CVE-2013-2141	The do_tkill function in kernel/signal.c in the Linux kernel before 3.8.9 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel memory via a crafted application that makes a (1) tkill or (2) tgkill system call.
CVE-2013-2175	HAProxy 1.4 before 1.4.24 and 1.5 before 1.5-dev19, when configured to use hdr_ip or other "hdr_*" functions with a negative occurrence count, allows remote attackers to cause a denial of service (negative array index usage and crash) via an HTTP header with a certain number of values, related to the MAX_HDR_HISTORY variable.
CVE-2013-2178	The apache-auth.conf, apache-nohome.conf, apache-noscript.conf, and apache-overflows.conf files in Fail2ban before 0.8.10 do not properly validate log messages, which allows remote attackers to block arbitrary IP addresses via certain messages in a request.
CVE-2013-2219	The Red Hat Directory Server before 8.2.11-13 and 389 Directory Server do not properly restrict access to entity attributes, which allows remote authenticated users to obtain sensitive information via a search query for the attribute.
CVE-2013-2232	The ip6_sk_dst_check function in net/ipv6/ip6_output.c in the Linux kernel before 3.10 allows local users to cause a denial of service (system crash) by using an AF_INET6 socket for a connection to an IPv4 interface.
CVE-2013-2234	The (1) key_notify_sa_flush and (2) key_notify_policy_flush functions in net/key/af_key.c in the Linux kernel before 3.10 do not initialize certain structure members, which allows local users to obtain sensitive information from kernel heap memory by reading a broadcast message from the notify interface of an IPSec key_socket.
CVE-2013-2266	libdns in ISC BIND 9.7.x and 9.8.x before 9.8.4-P2, 9.8.5 before 9.8.5b2, 9.9.x before 9.9.2-P2, and 9.9.3 before 9.9.3b2 on UNIX platforms allows

	remote attackers to cause a denial of service (memory consumption) via a crafted regular expression, as demonstrated by a memory-exhaustion attack against a machine running a named process.
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-2013-2375	Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors.
CVE-2013-2378	Unspecified vulnerability in Oracle MySQL 5.1.67 and earlier, 5.5.29 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via unknown vectors related to Information Schema.
CVE-2013-2383	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, 6 Update 43 and earlier, and 5.0 Update 41 and earlier; and OpenJDK 6 and 7; allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D, a different vulnerability than CVE-2013-1569, CVE-2013-2384, and CVE-2013-2420. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "handling of [a] glyph table" in the International Components for Unicode (ICU) Layout Engine before 51.2.
CVE-2013-2384	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, 6 Update 43 and earlier, and 5.0 Update 41 and earlier; and OpenJDK 6 and 7; allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D, a different vulnerability than CVE-2013-1569, CVE-2013-2383, and CVE-2013-2420. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "font layout" in the International Components for Unicode (ICU) Layout Engine before 51.2.
CVE-2013-2389	Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.
CVE-2013-2391	Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows

	local users to affect confidentiality and integrity via unknown vectors related to Server Install.
CVE-2013-2392	Unspecified vulnerability in Oracle MySQL 5.1.68 and earlier, 5.5.30 and earlier, and 5.6.10 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server Optimizer.
CVE-2013-2407	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier and 6 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality and availability via unknown vectors related to Libraries. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "XML security and the class loader."
CVE-2013-2412	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier and 6 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality via unknown vectors related to Serviceability. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to insufficient indication of an SSL connection failure by JConsole, related to RMI connection dialog box.
CVE-2013-2415	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, and OpenJDK 6 and 7, allows local users to affect confidentiality via vectors related to JAX-WS. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "processing of MTOM attachments" and the creation of temporary files with weak permissions.
CVE-2013-2417	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, 6 Update 43 and earlier, and 5.0 Update 41 and earlier; and OpenJDK 6 and 7; allows remote attackers to affect availability via unknown vectors related to Networking. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to an information leak involving InetAddress serialization. CVE has not investigated the apparent discrepancy between vendor reports regarding the impact of this issue.
CVE-2013-2419	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, 6 Update 43 and earlier, and 5.0 Update 41 and earlier; and OpenJDK 6 and 7; allows remote attackers to affect availability via

	unknown vectors related to 2D. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "font processing errors" in the International Components for Unicode (ICU) Layout Engine before 51.2.
CVE-2013-2420	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, 6 Update 43 and earlier, and 5.0 Update 41 and earlier; and OpenJDK 6 and 7; allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to insufficient "validation of images" in share/native/sun/awt/image/awt_ImageRep.c, possibly involving offsets.
CVE-2013-2421	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to HotSpot. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to incorrect MethodHandle lookups, which allows remote attackers to bypass Java sandbox restrictions.
CVE-2013-2422	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier and 6 Update 43 and earlier; and OpenJDK 6 and 7; allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to improper method-invocation restrictions by the MethodUtil trampoline class, which allows remote attackers to bypass the Java sandbox.
CVE-2013-2423	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, and OpenJDK 7, allows remote attackers to affect integrity via unknown vectors related to HotSpot. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from the original researcher that this vulnerability allows remote attackers to bypass permission checks by the MethodHandles method and modify arbitrary public final fields using reflection and type confusion, as demonstrated using integer and double fields to disable the security manager.

CVE-2013-2424	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, 6 Update 43 and earlier, and 5.0 Update 41 and earlier; and OpenJDK 6 and 7; allows remote attackers to affect confidentiality via vectors related to JMX. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "insufficient class access checks" when "creating new instances" using MBeanInstantiator.
CVE-2013-2426	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to incorrect invocation of the defaultReadObject method in the ConcurrentHashMap class, which allows remote attackers to bypass the Java sandbox.
CVE-2013-2429	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, 6 Update 43 and earlier, and 5.0 Update 41 and earlier; and OpenJDK 6 and 7; allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to ImageIO. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "JPEGImageWriter state corruption" when using native code, which triggers memory corruption.
CVE-2013-2430	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, 6 Update 43 and earlier, and 5.0 Update 41 and earlier; JavaFX 2.2.7 and earlier; and OpenJDK 6 and 7 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to ImageIO. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "JPEGImageReader state corruption" when using native code.
CVE-2013-2431	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, and OpenJDK 6 and 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to HotSpot. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to bypassing

	the Java sandbox using "method handle intrinsic frames."
CVE-2013-2436	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 17 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2013-1488 and CVE-2013-2426. NOTE: the previous information is from the April 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to incorrect "type checks" and "method handle binding" involving Wrapper.convert.
CVE-2013-2443	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality via unknown vectors related to Libraries, a different vulnerability than CVE-2013-2452 and CVE-2013-2455. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue is due to an incorrect "checking order" within the AccessControlContext class.
CVE-2013-2444	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier; JavaFX 2.2.21 and earlier; and OpenJDK 7 allows remote attackers to affect availability via vectors related to AWT. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue does not "properly manage and restrict certain resources related to the processing of fonts," possibly involving temporary files.
CVE-2013-2445	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect availability via unknown vectors related to Hotspot. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to bypass the Java sandbox via vectors related to "handling of memory allocation errors."
CVE-2013-2446	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality via vectors related to

	CORBA. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue does not properly enforce access restrictions for CORBA output streams.
CVE-2013-2447	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality via unknown vectors related to Networking. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to obtain a socket's local address via vectors involving inconsistencies between Socket.getLocalAddress and InetAddress.getLocalHost.
CVE-2013-2448	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Sound. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to bypass the Java sandbox via vectors related to insufficient "access restrictions" and "robustness of sound classes."
CVE-2013-2449	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality via unknown vectors related to Libraries. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to GnomeFileTypeDetector and a missing check for read permissions for a path.
CVE-2013-2450	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect availability via unknown vectors related to Serialization. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to improper handling of circular references in ObjectStreamClass.
CVE-2013-2452	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality via unknown

	vectors related to Libraries, a different vulnerability than CVE-2013-2443 and CVE-2013-2455. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to "network address handling in virtual machine identifiers" and the lack of "unique and unpredictable IDs" in the java.rmi.dgc.VMID class.
CVE-2013-2453	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier and 6 Update 45 and earlier allows remote attackers to affect integrity via vectors related to JMX. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue is due to a missing check for "package access" by the MBeanServer Introspector.
CVE-2013-2454	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality and integrity via vectors related to JDBC. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue does not properly restrict access to certain class packages in the SerialJavaObject class, which allows remote attackers to bypass the Java sandbox.
CVE-2013-2455	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality via unknown vectors related to Libraries, a different vulnerability than CVE-2013-2443 and CVE-2013-2452. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to incorrect access checks by the (1) getEnclosingClass, (2) getEnclosingMethod, and (3) getEnclosingConstructor methods.
CVE-2013-2456	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality via unknown vectors related to Serialization. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue is related to improper access checks for subclasses in the ObjectOutputStream class.
CVE-2013-2457	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7

	Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect integrity via vectors related to JMX. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue is due to an incorrect implementation of "certain class checks" that allows remote attackers to bypass intended class restrictions.
CVE-2013-2458	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality and integrity via unknown vectors related to Libraries. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to bypass the Java sandbox via "an error related to method handles."
CVE-2013-2459	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to AWT. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to bypass the Java sandbox via vectors related to "integer overflow checks."
CVE-2013-2460	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Serviceability. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to bypass the Java sandbox via vectors related to "insufficient access checks" in the tracing component.
CVE-2013-2461	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier and 6 Update 45 and earlier; the Oracle JRockit component in Oracle Fusion Middleware R27.7.5 and earlier and R28.2.7 and earlier; and OpenJDK 7 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries. NOTE: the previous information is from the June and July 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to bypass verification of XML signatures via vectors related to a "Missing check for [a] valid

	DOMCanonicalizationMethod canonicalization algorithm."
CVE-2013-2463	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to bypass the Java sandbox via vectors related to "Incorrect image attribute verification" in 2D.
CVE-2013-2465	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to bypass the Java sandbox via vectors related to "Incorrect image channel verification" in 2D.
CVE-2013-2469	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to bypass the Java sandbox via vectors related to "Incorrect image layout verification" in 2D.
CVE-2013-2470	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to bypass the Java sandbox via vectors related to "ImagingLib byte lookup processing."
CVE-2013-2471	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality, integrity, and

	availability via unknown vectors related to 2D. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to bypass the Java sandbox via vectors related to "Incorrect IntegerComponentRaster size checks."
CVE-2013-2472	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to bypass the Java sandbox via vectors related to "Incorrect ShortBandedRaster size checks" in 2D.
CVE-2013-2473	Unspecified vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 21 and earlier, 6 Update 45 and earlier, and 5.0 Update 45 and earlier, and OpenJDK 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D. NOTE: the previous information is from the June 2013 CPU. Oracle has not commented on claims from another vendor that this issue allows remote attackers to bypass the Java sandbox via vectors related to "Incorrect ByteBandedRaster size checks" in 2D.
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-2013-2561	OpenFabrics ibutils 1.5.7 allows local users to overwrite arbitrary files via a symlink attack on (1) ibdiagnet.db, (2) ibdiagnet.fdbs, (3) ibdiagnet_ibis.log, (4) ibdiagnet.log, (5) ibdiagnet.lst, (6) ibdiagnet.mcfdbs, (7) ibdiagnet.pkey, (8) ibdiagnet.psl, (9) ibdiagnet.slvl, or (10) ibdiagnet.sm in /tmp/.
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-2013-2634	net/dcb/dcbnl.c in the Linux kernel before 3.8.4 does not initialize certain structures, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.
CVE-2013-2635	The rtnl_fill_ifinfo function in net/core/rtnetlink.c in the Linux kernel before 3.8.4 does not initialize a certain structure member, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.
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-2013-2741	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-2013-2776	sudo 1.3.5 through 1.7.10p5 and 1.8.0 through 1.8.6p6, when running on systems without /proc or the sysctl function with the tty_tickets option enabled, does not properly validate the controlling terminal device, which allows local users with sudo permissions to hijack the authorization of another terminal via vectors related to connecting to the standard input, output, and error file descriptors of another terminal. NOTE: this is one of three closely-related vulnerabilities that were originally assigned CVE-2013-1776, but they have been SPLIT because of different affected versions.
CVE-2013-2777	sudo before 1.7.10p5 and 1.8.x before 1.8.6p6, when the tty_tickets option is enabled, does not properly validate the controlling terminal device, which allows local users with sudo permissions to hijack the authorization of another terminal via vectors related to a session without a controlling terminal device and connecting to the standard input, output, and error file descriptors of another terminal. NOTE: this is one of three closely-related vulnerabilities that were originally assigned CVE-2013-1776, but they have been SPLIT because of different affected versions.
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-2013-2852	Format string vulnerability in the b43_request_firmware function in drivers/net/wireless/b43/main.c in the

	Broadcom B43 wireless driver in the Linux kernel through 3.9.4 allows local users to gain privileges by leveraging root access and including format string specifiers in an fwpostfix modprobe parameter, leading to improper construction of an error message.
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-2013-3222	The vcc_recvmsg function in net/atm/common.c in the Linux kernel before 3.9-rc7 does not initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.
CVE-2013-3224	The bt_sock_recvmsg function in net/bluetooth/af_bluetooth.c in the Linux kernel before 3.9-rc7 does not properly initialize a certain length variable, which allows local users to obtain sensitive information from

	kernel stack memory via a crafted recvmsg or recvfrom system call.
CVE-2013-3225	The rfcomm_sock_recvmsg function in net/bluetooth/rfcomm/sock.c in the Linux kernel before 3.9-rc7 does not initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.
CVE-2013-3231	The llc_ui_recvmsg function in net/llc/af_llc.c in the Linux kernel before 3.9-rc7 does not initialize a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.
CVE-2013-3235	net/tipc/socket.c in the Linux kernel before 3.9-rc7 does not initialize a certain data structure and a certain length variable, which allows local users to obtain sensitive information from kernel stack memory via a crafted recvmsg or recvfrom system call.
CVE-2013-3301	The ftrace implementation in the Linux kernel before 3.8.8 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by leveraging the CAP_SYS_ADMIN capability for write access to the (1) set_ftrace_pid or (2) set_graph_function file, and then making an lseek system call.
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-2013-3557	The dissect_ber_choice function in epan/dissectors/packet-ber.c in the ASN.1 BER dissector in Wireshark 1.6.x before 1.6.15 and 1.8.x before 1.8.7 does not properly initialize a certain variable, which allows remote attackers to cause a denial of service (application crash) via a malformed packet.
CVE-2013-3559	epan/dissectors/packet-dcp-etsi.c in the DCP ETSI dissector in Wireshark 1.8.x before 1.8.7 uses incorrect integer data types, which allows remote attackers to cause a denial of service (integer overflow, and heap memory corruption or NULL pointer dereference, and application crash) via a malformed packet.
CVE-2013-3561	Multiple integer overflows in Wireshark 1.8.x before 1.8.7 allow remote attackers to cause a denial of service (loop or application crash) via a malformed packet, related to a crash of the Websocket dissector, an infinite loop in the MySQL dissector, and a large loop in the ETCH dissector.
CVE-2013-3567	Puppet 2.7.x before 2.7.22 and 3.2.x before 3.2.2, and Puppet Enterprise before 2.8.2, deserializes untrusted YAML, which allows remote attackers to instantiate arbitrary Ruby classes and execute arbitrary code via a crafted REST API call.
CVE-2013-3571	socat 1.2.0.0 before 1.7.2.2 and 2.0.0-b1 before 2.0.0-b6, when used for a listen type address and the fork option is enabled, allows remote attackers to cause a denial of service (file descriptor consumption) via multiple request that are refused based on the (1) sourceport, (2) lowport, (3) range, or (4) tcpwrap restrictions.
CVE-2013-3829	Unspecified vulnerability in the Java SE, Java SE Embedded component in Oracle Java SE Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality and integrity via unknown vectors related to Libraries.
CVE-2013-3839	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.70 and earlier, 5.5.32 and earlier, and 5.6.12 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.
CVE-2013-4002	Unspecified vulnerability in the Java Runtime Environment (JRE) in IBM Java 5.0 before 5.0 SR16-FP3, 6 before 6 SR14, 6.0.1 before 6.0.1 SR6, and 7 before 7 SR5 allows remote attackers to affect availability via unknown vectors.
CVE-2013-4075	epan/dissectors/packet-gmr1_bcch.c in the GMR-1 BCCH dissector in Wireshark 1.8.x before 1.8.8 does

	not properly initialize memory, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.
CVE-2013-4081	The http_payload_subdissector function in epan/dissectors/packet-http.c in the HTTP dissector in Wireshark 1.6.x before 1.6.16 and 1.8.x before 1.8.8 does not properly determine when to use a recursive approach, which allows remote attackers to cause a denial of service (stack consumption) via a crafted packet.
CVE-2013-4083	The dissect_pft function in epan/dissectors/packet-dcp-etsi.c in the DCP ETSI dissector in Wireshark 1.6.x before 1.6.16, 1.8.x before 1.8.8, and 1.10.0 does not validate a certain fragment length value, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.
CVE-2013-4113	ext/xml/xml.c in PHP before 5.3.27 does not properly consider parsing depth, which allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a crafted document that is processed by the xml_parse_into_struct function.
CVE-2013-4115	Buffer overflow in the idnsALookup function in dns_internal.cc in Squid 3.2 through 3.2.11 and 3.3 through 3.3.6 allows remote attackers to cause a denial of service (memory corruption and server termination) via a long name in a DNS lookup request.
CVE-2013-4122	Cyrus SASL 2.1.23, 2.1.26, and earlier does not properly handle when a NULL value is returned upon an error by the crypt function as implemented in glibc 2.17 and later, which allows remote attackers to cause a denial of service (thread crash and consumption) via (1) an invalid salt or, when FIPS-140 is enabled, a (2) DES or (3) MD5 encrypted password, which triggers a NULL pointer dereference.
CVE-2013-4131	The mod_dav_svn Apache HTTPD server module in Subversion 1.7.0 through 1.7.10 and 1.8.x before 1.8.1 allows remote authenticated users to cause a denial of service (assertion failure or out-of-bounds read) via a certain (1) COPY, (2) DELETE, or (3) MOVE request against a revision root.
CVE-2013-4162	The udp_v6_push_pending_frames function in net/ipv6/udp.c in the IPv6 implementation in the Linux kernel through 3.10.3 makes an incorrect function call for pending data, which allows local users to cause a denial of service (BUG and system crash) via a crafted application that uses the UDP_CORK option in a setsockopt system call.
CVE-2013-4164	Heap-based buffer overflow in Ruby 1.8, 1.9 before 1.9.3-p484, 2.0 before 2.0.0-p353, 2.1 before 2.1.0

	preview2, and trunk before revision 43780 allows context-dependent attackers to cause a denial of service (segmentation fault) and possibly execute arbitrary code via a string that is converted to a floating point value, as demonstrated using (1) the to_f method or (2) JSON.parse.
CVE-2013-4214	rss-newsfeed.php in Nagios Core 3.4.4, 3.5.1, and earlier, when MAGPIE_CACHE_ON is set to 1, allows local users to overwrite arbitrary files via a symlink attack on /tmp/magpie_cache.
CVE-2013-4231	Multiple buffer overflows in libtiff before 4.0.3 allow remote attackers to cause a denial of service (out-of-bounds write) via a crafted (1) extension block in a GIF image or (2) GIF raster image to tools/gif2tiff.c or (3) a long filename for a TIFF image to tools/rgb2ycbcr.c. NOTE: vectors 1 and 3 are disputed by Red Hat, which states that the input cannot exceed the allocated buffer size.
CVE-2013-4232	Use-after-free vulnerability in the t2p_readwrite_pdf_image function in tools/tiff2pdf.c in libtiff 4.0.3 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted TIFF image.
CVE-2013-4238	The ssl.match_hostname function in the SSL module in Python 2.6 through 3.4 does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.
CVE-2013-4242	GnuPG before 1.4.14, and Libgcrypt before 1.5.3 as used in GnuPG 2.0.x and possibly other products, allows local users to obtain private RSA keys via a cache side-channel attack involving the L3 cache, aka Flush+Reload.
CVE-2013-4243	Heap-based buffer overflow in the readgifimage function in the gif2tiff tool in libtiff 4.0.3 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted height and width values in a GIF image.
CVE-2013-4244	The LZW decompressor in the gif2tiff tool in libtiff 4.0.3 and earlier allows context-dependent attackers to cause a denial of service (out-of-bounds write and crash) or possibly execute arbitrary code via a crafted GIF image.
CVE-2013-4248	The openssl_x509_parse function in openssl.c in the OpenSSL module in PHP before 5.4.18 and 5.5.x before 5.5.2 does not properly handle a '\0' character in a domain name in the Subject Alternative Name field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted

	certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.
CVE-2013-4251	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2013-4283	ns-slapd in 389 Directory Server before 1.3.0.8 allows remote attackers to cause a denial of service (server crash) via a crafted Distinguished Name (DN) in a MOD operation request.
CVE-2013-4286	Apache Tomcat before 6.0.39, 7.x before 7.0.47, and 8.x before 8.0.0-RC3, when an HTTP connector or AJP connector is used, does not properly handle certain inconsistent HTTP request headers, which allows remote attackers to trigger incorrect identification of a request's length and conduct request-smuggling attacks via (1) multiple Content-Length headers or (2) a Content-Length header and a "Transfer-Encoding: chunked" header. NOTE: this vulnerability exists because of an incomplete fix for CVE-2005-2090.
CVE-2013-4287	Algorithmic complexity vulnerability in Gem::Version::VERSION_PATTERN in lib/rubygems/version.rb in RubyGems before 1.8.23.1, 1.8.24 through 1.8.25, 2.0.x before 2.0.8, and 2.1.x before 2.1.0, as used in Ruby 1.9.0 through 2.0.0p247, allows remote attackers to cause a denial of service (CPU consumption) via a crafted gem version that triggers a large amount of backtracking in a regular expression.
CVE-2013-4299	Interpretation conflict in drivers/md/dm-snap-persistent.c in the Linux kernel through 3.11.6 allows remote authenticated users to obtain sensitive information or modify data via a crafted mapping to a snapshot block device.
CVE-2013-4312	The Linux kernel before 4.4.1 allows local users to bypass file-descriptor limits and cause a denial of service (memory consumption) by sending each descriptor over a UNIX socket before closing it, related to net/unix/af_unix.c and net/unix/garbage.c.
CVE-2013-4322	Apache Tomcat before 6.0.39, 7.x before 7.0.50, and 8.x before 8.0.0-RC10 processes chunked transfer coding without properly handling (1) a large total amount of chunked data or (2) whitespace characters in an HTTP header value within a trailer field, which allows remote attackers to cause a denial of service by streaming data. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-3544.
CVE-2013-4332	Multiple integer overflows in malloc/malloc.c in the GNU C Library (aka glibc or libc6) 2.18 and earlier

	allow context-dependent attackers to cause a denial of service (heap corruption) via a large value to the (1) pvalloc, (2) valloc, (3) posix_memalign, (4) memalign, or (5) aligned_alloc functions.
CVE-2013-4342	xinetd does not enforce the user and group configuration directives for TCPMUX services, which causes these services to be run as root and makes it easier for remote attackers to gain privileges by leveraging another vulnerability in a service.
CVE-2013-4346	The Server.verify_request function in SimpleGeo python-oauth2 does not check the nonce, which allows remote attackers to perform replay attacks via a signed URL.
CVE-2013-4347	The (1) make_nonce, (2) generate_nonce, and (3) generate_verifier functions in SimpleGeo python-oauth2 uses weak random numbers to generate nonces, which makes it easier for remote attackers to guess the nonce via a brute force attack.
CVE-2013-4348	The skb_flow_dissect function in net/core/flow_dissector.c in the Linux kernel through 3.12 allows remote attackers to cause a denial of service (infinite loop) via a small value in the IHL field of a packet with IPIP encapsulation.
CVE-2013-4351	GnuPG 1.4.x, 2.0.x, and 2.1.x treats a key flags subpacket with all bits cleared (no usage permitted) as if it has all bits set (all usage permitted), which might allow remote attackers to bypass intended cryptographic protection mechanisms by leveraging the subkey.
CVE-2013-4353	The ssl3_take_mac function in ssl/s3_both.c in OpenSSL 1.0.1 before 1.0.1f allows remote TLS servers to cause a denial of service (NULL pointer dereference and application crash) via a crafted Next Protocol Negotiation record in a TLS handshake.
CVE-2013-4363	Algorithmic complexity vulnerability in Gem::Version::ANCHORED_VERSION_PATTERN in lib/rubygems/version.rb in RubyGems before 1.8.23.2, 1.8.24 through 1.8.26, 2.0.x before 2.0.10, and 2.1.x before 2.1.5, as used in Ruby 1.9.0 through 2.0.0p247, allows remote attackers to cause a denial of service (CPU consumption) via a crafted gem version that triggers a large amount of backtracking in a regular expression. NOTE: this issue is due to an incomplete fix for CVE-2013-4287.
CVE-2013-4365	Heap-based buffer overflow in the fcgid_header_bucket_read function in fcgid_bucket.c in the mod_fcgid module before 2.3.9 for the Apache HTTP Server allows remote attackers to have an unspecified impact via unknown vectors.

CVE-2013-4387	net/ipv6/ip6_output.c in the Linux kernel through 3.11.4 does not properly determine the need for UDP Fragmentation Offload (UFO) processing of small packets after the UFO queueing of a large packet, which allows remote attackers to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact via network traffic that triggers a large response packet.
CVE-2013-4396	Use-after-free vulnerability in the doImageText function in dix/dixfonts.c in the xorg-server module before 1.14.4 in X.Org X11 allows remote authenticated users to cause a denial of service (daemon crash) or possibly execute arbitrary code via a crafted ImageText request that triggers memory-allocation failure.
CVE-2013-4402	The compressed packet parser in GnuPG 1.4.x before 1.4.15 and 2.0.x before 2.0.22 allows remote attackers to cause a denial of service (infinite recursion) via a crafted OpenPGP message.
CVE-2013-4449	The rwm overlay in OpenLDAP 2.4.23, 2.4.36, and earlier does not properly count references, which allows remote attackers to cause a denial of service (slapd crash) by unbinding immediately after a search request, which triggers rwm_conn_destroy to free the session context while it is being used by rwm_op_search.
CVE-2013-4470	The Linux kernel before 3.12, when UDP Fragmentation Offload (UFO) is enabled, does not properly initialize certain data structures, which allows local users to cause a denial of service (memory corruption and system crash) or possibly gain privileges via a crafted application that uses the UDP_CORK option in a setsockopt system call and sends both short and long packets, related to the ip_ufo_append_data function in net/ipv4/ip_output.c and the ip6_ufo_append_data function in net/ipv6/ip6_output.c.
CVE-2013-4484	Varnish before 3.0.5 allows remote attackers to cause a denial of service (child-process crash and temporary caching outage) via a GET request with trailing whitespace characters and no URI.
CVE-2013-4485	389 Directory Server 1.2.11.15 (aka Red Hat Directory Server before 8.2.11-14) allows remote authenticated users to cause a denial of service (crash) via multiple @ characters in a GER attribute list in a search request.
CVE-2013-4505	The is_this_legal function in mod_dontdothat for Apache Subversion 1.4.0 through 1.7.13 and 1.8.0 through 1.8.4 allows remote attackers to bypass intended access restrictions and possibly cause a denial of service (resource consumption) via a relative URL in a REPORT request.
CVE-2013-4508	lighttpd before 1.4.34, when SNI is enabled, configures weak SSL ciphers, which makes it easier for remote

	attackers to hijack sessions by inserting packets into the client-server data stream or obtain sensitive information by sniffing the network.
CVE-2013-4547	nginx 0.8.41 through 1.4.3 and 1.5.x before 1.5.7 allows remote attackers to bypass intended restrictions via an unescaped space character in a URI.
CVE-2013-4558	The get_parent_resource function in repos.c in mod_dav_svn Apache HTTPD server module in Subversion 1.7.11 through 1.7.13 and 1.8.1 through 1.8.4, when built with assertions enabled and SVNAutoversioning is enabled, allows remote attackers to cause a denial of service (assertion failure and Apache process abort) via a non-canonical URL in a request, as demonstrated using a trailing /.
CVE-2013-4559	lighttpd before 1.4.33 does not check the return value of the (1) setuid, (2) setgid, or (3) setgroups functions, which might cause lighttpd to run as root if it is restarted and allows remote attackers to gain privileges, as demonstrated by multiple calls to the clone function that cause setuid to fail when the user process limit is reached.
CVE-2013-4560	Use-after-free vulnerability in lighttpd before 1.4.33 allows remote attackers to cause a denial of service (segmentation fault and crash) via unspecified vectors that trigger FAMMonitorDirectory failures.
CVE-2013-4566	mod_nss 1.0.8 and earlier, when NSSVerifyClient is set to none for the server/vhost context, does not enforce the NSSVerifyClient setting in the directory context, which allows remote attackers to bypass intended access restrictions.
CVE-2013-4576	GnuPG 1.x before 1.4.16 generates RSA keys using sequences of introductions with certain patterns that introduce a side channel, which allows physically proximate attackers to extract RSA keys via a chosen-ciphertext attack and acoustic cryptanalysis during decryption. NOTE: applications are not typically expected to protect themselves from acoustic side-channel attacks, since this is arguably the responsibility of the physical device. Accordingly, issues of this type would not normally receive a CVE identifier. However, for this issue, the developer has specified a security policy in which GnuPG should offer side-channel resistance, and developer-specified security-policy violations are within the scope of CVE.
CVE-2013-4588	Multiple stack-based buffer overflows in net/netfilter/ipvs/ip_vs_ctl.c in the Linux kernel before 2.6.33, when CONFIG_IP_VS is used, allow local users to gain privileges by leveraging the CAP_NET_ADMIN capability for (1) a getsockopt system call, related to the

	do_ip_vs_get_ctl function, or (2) a setsockopt system call, related to the do_ip_vs_set_ctl function.
CVE-2013-4761	Unspecified vulnerability in Puppet 2.7.x before 2.7.23 and 3.2.x before 3.2.4, and Puppet Enterprise 2.8.x before 2.8.3 and 3.0.x before 3.0.1, allows remote attackers to execute arbitrary Ruby programs from the master via the resource_type service. NOTE: this vulnerability can only be exploited utilizing unspecified "local file system access" to the Puppet Master.
CVE-2013-4854	The RFC 5011 implementation in rdata.c in ISC BIND 9.7.x and 9.8.x before 9.8.5-P2, 9.8.6b1, 9.9.x before 9.9.3-P2, and 9.9.4b1, and DNSco BIND 9.9.3-S1 before 9.9.3-S1-P1 and 9.9.4-S1b1, allows remote attackers to cause a denial of service (assertion failure and named daemon exit) via a query with a malformed RDATA section that is not properly handled during construction of a log message, as exploited in the wild in July 2013.
CVE-2013-4885	The http-domino-enum-passwords.nse script in NMap before 6.40, when domino-enum-passwords.idpath is set, allows remote servers to upload "arbitrarily named" files via a crafted FullName parameter in a response, as demonstrated using directory traversal sequences.
CVE-2013-4927	Integer signedness error in the get_type_length function in epan/dissectors/packet-btsdp.c in the Bluetooth SDP dissector in Wireshark 1.8.x before 1.8.9 and 1.10.x before 1.10.1 allows remote attackers to cause a denial of service (loop and CPU consumption) via a crafted packet.
CVE-2013-4931	epan/proto.c in Wireshark 1.8.x before 1.8.9 and 1.10.x before 1.10.1 allows remote attackers to cause a denial of service (loop) via a crafted packet that is not properly handled by the GSM RR dissector.
CVE-2013-4932	Multiple array index errors in epan/dissectors/packet-gsm_a_common.c in the GSM A Common dissector in Wireshark 1.8.x before 1.8.9 and 1.10.x before 1.10.1 allow remote attackers to cause a denial of service (application crash) via a crafted packet.
CVE-2013-4933	The netmon_open function in wiretap/netmon.c in the Netmon file parser in Wireshark 1.8.x before 1.8.9 and 1.10.x before 1.10.1 does not properly allocate memory, which allows remote attackers to cause a denial of service (application crash) via a crafted packet-trace file.
CVE-2013-4934	The netmon_open function in wiretap/netmon.c in the Netmon file parser in Wireshark 1.8.x before 1.8.9 and 1.10.x before 1.10.1 does not initialize certain structure members, which allows remote attackers to cause a denial of service (application crash) via a crafted packet-trace file.

CVE-2013-4935	The dissect_per_length_determinant function in epan/dissectors/packet-per.c in the ASN.1 PER dissector in Wireshark 1.8.x before 1.8.9 and 1.10.x before 1.10.1 does not initialize a length field in certain abnormal situations, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.
CVE-2013-4936	The IsDFP_Frame function in plugins/profinet/packet-pn-rt.c in the PROFINET Real-Time dissector in Wireshark 1.10.x before 1.10.1 does not validate MAC addresses, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted packet.
CVE-2013-4956	Puppet Module Tool (PMT), as used in Puppet 2.7.x before 2.7.23 and 3.2.x before 3.2.4, and Puppet Enterprise 2.8.x before 2.8.3 and 3.0.x before 3.0.1, installs modules with weak permissions if those permissions were used when the modules were originally built, which might allow local users to read or modify those modules depending on the original permissions.
CVE-2013-4969	Puppet before 3.3.3 and 3.4 before 3.4.1 and Puppet Enterprise (PE) before 2.8.4 and 3.1 before 3.1.1 allows local users to overwrite arbitrary files via a symlink attack on unspecified files.
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-2013-5588	Multiple cross-site scripting (XSS) vulnerabilities in Cacti 0.8.8b and earlier allow remote attackers to inject arbitrary web script or HTML via (1) the step parameter to install/index.php or (2) the id parameter to cacti/host.php.
CVE-2013-5589	SQL injection vulnerability in cacti/host.php in Cacti 0.8.8b and earlier allows remote attackers to execute arbitrary SQL commands via the id parameter.
CVE-2013-5605	Mozilla Network Security Services (NSS) 3.14 before 3.14.5 and 3.15 before 3.15.3 allows remote attackers to cause a denial of service or possibly have unspecified other impact via invalid handshake packets.
CVE-2013-5606	The CERT_VerifyCert function in lib/certhigh/certvfy.c in Mozilla Network Security Services (NSS) 3.15 before 3.15.3 provides an unexpected return value for an incompatible key-usage certificate when the CERTVerifyLog argument is valid, which might allow remote attackers to bypass intended access restrictions via a crafted certificate.
CVE-2013-5607	Integer overflow in the PL_ArenaAllocate function in Mozilla Netscape Portable Runtime (NSPR) before 4.10.2, as used in Firefox before 25.0.1, Firefox ESR 17.x before 17.0.11 and 24.x before 24.1.1, and SeaMonkey before 2.22.1, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted X.509 certificate, a related issue to CVE-2013-1741.
CVE-2013-5653	The getenv and filenameforall functions in Ghostscript 9.10 ignore the "-dSAFER" argument, which allows remote attackers to read data via a crafted postscript file.
CVE-2013-5704	The mod_headers module in the Apache HTTP Server 2.2.22 allows remote attackers to bypass "RequestHeader unset" directives by placing a header

	in the trailer portion of data sent with chunked transfer coding. NOTE: the vendor states "this is not a security issue in httpd as such."
CVE-2013-5705	apache2/modsecurity.c in ModSecurity before 2.7.6 allows remote attackers to bypass rules by using chunked transfer coding with a capitalized Chunked value in the Transfer-Encoding HTTP header.
CVE-2013-5721	The dissect_mq_rr function in epan/dissectors/packet-mq.c in the MQ dissector in Wireshark 1.8.x before 1.8.10 and 1.10.x before 1.10.2 does not properly determine when to enter a certain loop, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.
CVE-2013-5772	Unspecified vulnerability in the Java SE component in Oracle Java SE Java SE 7u40 and earlier and Java SE 6u60 and earlier allows remote attackers to affect integrity via unknown vectors related to jhat.
CVE-2013-5774	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, 6u60 and earlier, 5.0u51 and earlier, and Embedded 7u40 and earlier allows remote attackers to affect integrity via unknown vectors related to Libraries.
CVE-2013-5778	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, 6u60 and earlier, 5.0u51 and earlier, and Embedded 7u40 and earlier allows remote attackers to affect confidentiality via unknown vectors related to 2D.
CVE-2013-5780	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, JRockit R28.2.8 and earlier, JRockit R27.7.6 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality via unknown vectors related to Libraries.
CVE-2013-5782	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, JRockit R28.2.8 and earlier, JRockit R27.7.6 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.
CVE-2013-5783	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality and integrity via unknown vectors related to Swing.
CVE-2013-5784	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect integrity via vectors related to SCRIPTING.
CVE-2013-5790	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and

	earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality via vectors related to BEANS.
CVE-2013-5797	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, JRockit R28.2.8 and earlier, JRockit R27.7.6 and earlier, and JavaFX 2.2.40 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Javadoc.
CVE-2013-5800	Unspecified vulnerability in Oracle Java SE 7u40 and earlier and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality via vectors related to JGSS.
CVE-2013-5802	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, JRockit R28.2.8 and earlier, JRockit R27.7.6 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JAXP.
CVE-2013-5803	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, JRockit R28.2.8 and earlier, JRockit R27.7.6 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect availability via vectors related to JGSS.
CVE-2013-5804	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, JRockit R28.2.8 and earlier, and JRockit R27.7.6 and earlier allows remote attackers to affect confidentiality and integrity via unknown vectors related to Javadoc.
CVE-2013-5809	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D, a different vulnerability than CVE-2013-5829.
CVE-2013-5814	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality, integrity, and availability via vectors related to CORBA.
CVE-2013-5817	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JNDI.
CVE-2013-5820	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, and Java SE

	Embedded 7u40 and earlier allows remote attackers to affect integrity via vectors related to JAX-WS.
CVE-2013-5823	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, JRockit R28.2.8 and earlier, JRockit R27.7.6 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect availability via unknown vectors related to Security.
CVE-2013-5825	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, JRockit R28.2.8 and earlier, JRockit R27.7.6 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect availability via vectors related to JAXP.
CVE-2013-5829	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D, a different vulnerability than CVE-2013-5809.
CVE-2013-5830	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, JRockit R28.2.8 and earlier, JRockit R27.7.6 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.
CVE-2013-5838	Unspecified vulnerability in Oracle Java SE 7u25 and earlier, and Java SE Embedded 7u25 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.
CVE-2013-5840	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality via unknown vectors related to Libraries.
CVE-2013-5842	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2013-5850.
CVE-2013-5849	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality via vectors related to AWT.
CVE-2013-5850	Unspecified vulnerability in Oracle Java SE 7u40 and earlier, Java SE 6u60 and earlier, Java SE 5.0u51 and

	earlier, and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2013-5842.
CVE-2013-5851	Unspecified vulnerability in Oracle Java SE 7u40 and earlier and Java SE Embedded 7u40 and earlier allows remote attackers to affect confidentiality via vectors related to JAXP.
CVE-2013-5878	Unspecified vulnerability in Oracle Java SE 6u65 and 7u45, Java SE Embedded 7u45, and OpenJDK 7 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Security. NOTE: the previous information is from the January 2014 CPU. Oracle has not commented on third-party claims that the Security component does not properly handle null XML namespace (xmlns) attributes during XML document canonicalization, which allows attackers to escape the sandbox.
CVE-2013-5884	Unspecified vulnerability in Oracle Java SE 5.0u55, 6u65, and 7u45; Java SE Embedded 7u45; and OpenJDK 7 allows remote attackers to affect confidentiality via vectors related to CORBA. NOTE: the previous information is from the January 2014 CPU. Oracle has not commented on third-party claims that the issue is related to an incorrect check for code permissions by CORBA stub factories.
CVE-2013-5893	Unspecified vulnerability in Oracle Java SE 7u45 and Java SE Embedded 7u45, and OpenJDK 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries. NOTE: the previous information is from the January 2014 CPU. Oracle has not commented on third-party claims that the issue is related to improper handling of methods in MethodHandles in HotSpot JVM, which allows attackers to escape the sandbox.
CVE-2013-5896	Unspecified vulnerability in Oracle Java SE 5.0u55, 6u65, and 7u45; Java SE Embedded 7u45; and OpenJDK 7 allows remote attackers to affect availability via vectors related to CORBA. NOTE: the previous information is from the January 2014 CPU. Oracle has not commented on third-party claims that com.sun.corba.se and its sub-packages are not included on the restricted package list.
CVE-2013-5907	Unspecified vulnerability in Oracle Java SE 5.0u55, 6u65, and 7u45; JRockit R27.7.7 and R28.2.9; Java SE Embedded 7u45; and OpenJDK 7 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D. NOTE: the previous information is from the January 2014 CPU. Oracle has not commented on third-party claims that the issue is due to incorrect input validation in

	LookupProcessor.cpp in the ICU Layout Engine, which allows attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted font file.
CVE-2013-5908	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.72 and earlier, 5.5.34 and earlier, and 5.6.14 and earlier allows remote attackers to affect availability via unknown vectors related to Error Handling.
CVE-2013-5910	Unspecified vulnerability in Oracle Java SE 6u65 and 7u45, Java SE Embedded 7u45, and OpenJDK 7 allows remote attackers to affect integrity via unknown vectors related to Security. NOTE: the previous information is from the January 2014 CPU. Oracle has not commented on third-party claims that CanonicalizerBase.java in the XML canonicalizer allows untrusted code to access mutable byte arrays.
CVE-2013-6045	Multiple heap-based buffer overflows in OpenJPEG 1.3 and earlier might allow remote attackers to execute arbitrary code via unspecified vectors.
CVE-2013-6048	The get_group_tree function in lib/Munin/Master/HTMLConfig.pm in Munin before 2.0.18 allows remote nodes to cause a denial of service (infinite loop and memory consumption in the munin-html process) via crafted multigraph data.
CVE-2013-6051	The bgp_attr_unknown function in bgp_attr.c in Quagga 0.99.21 does not properly initialize the total variable, which allows remote attackers to cause a denial of service (bgpd crash) via a crafted BGP update.
CVE-2013-6052	OpenJPEG 1.3 and earlier allows remote attackers to obtain sensitive information via unspecified vectors that trigger a heap-based out-of-bounds read.
CVE-2013-6054	Heap-based buffer overflow in OpenJPEG 1.3 has unspecified impact and remote vectors, a different vulnerability than CVE-2013-6045.
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-2013-6336	The ieee802154_map_rec function in epan/dissectors/packet-ieee802154.c in the IEEE 802.15.4 dissector in Wireshark 1.8.x before 1.8.11 and 1.10.x before 1.10.3 uses an incorrect pointer chain, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.
CVE-2013-6337	Unspecified vulnerability in the NBAP dissector in Wireshark 1.8.x before 1.8.11 and 1.10.x before 1.10.3

	allows remote attackers to cause a denial of service (application crash) via a crafted packet.
CVE-2013-6338	The dissect_sip_common function in epan/dissectors/packet-sip.c in the SIP dissector in Wireshark 1.8.x before 1.8.11 and 1.10.x before 1.10.3 does not properly initialize a data structure, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.
CVE-2013-6339	The dissect_openwire_type function in epan/dissectors/packet-openwire.c in the OpenWire dissector in Wireshark 1.8.x before 1.8.11 and 1.10.x before 1.10.3 allows remote attackers to cause a denial of service (loop) via a crafted packet.
CVE-2013-6340	epan/dissectors/packet-tcp.c in the TCP dissector in Wireshark 1.8.x before 1.8.11 and 1.10.x before 1.10.3 does not properly determine the amount of remaining data, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.
CVE-2013-6359	Munin::Master::Node in Munin before 2.0.18 allows remote attackers to cause a denial of service (abort data collection for node) via a plugin that uses "multigraph" as a multigraph service name.
CVE-2013-6369	Stack-based buffer overflow in the jbg_dec_in function in libjbig/jbig.c in JBIG-KIT before 2.1 allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code via a crafted image file.
CVE-2013-6370	Buffer overflow in the printbuf APIs in json-c before 0.12 allows remote attackers to cause a denial of service via unspecified vectors.
CVE-2013-6371	The hash functionality in json-c before 0.12 allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted JSON data, involving collisions.
CVE-2013-6382	Multiple buffer underflows in the XFS implementation in the Linux kernel through 3.12.1 allow local users to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging the CAP_SYS_ADMIN capability for a (1) XFS_IOC_ATTRLIST_BY_HANDLE or (2) XFS_IOC_ATTRLIST_BY_HANDLE_32 ioctl call with a crafted length value, related to the xfs_attrlist_by_handle function in fs/xfs/xfs_ioctl.c and the xfs_compat_attrlist_by_handle function in fs/xfs/xfs_ioctl32.c.
CVE-2013-6393	The yaml_parser_scan_tag_uri function in scanner.c in LibYAML before 0.1.5 performs an incorrect cast, which allows remote attackers to cause a denial of service (application crash) and possibly execute arbitrary code

	via crafted tags in a YAML document, which triggers a heap-based buffer overflow.
CVE-2013-6395	Cross-site scripting (XSS) vulnerability in header.php in Ganglia Web 3.5.8 and 3.5.10 allows remote attackers to inject arbitrary web script or HTML via the host_regex parameter to the default URI, which is processed by get_context.php.
CVE-2013-6412	The transform_save function in transform.c in Augeas 1.0.0 through 1.1.0 does not properly calculate the permission values when the umask contains a "7," which causes world-writable permissions to be used for new files and allows local users to modify the files via unspecified vectors.
CVE-2013-6420	The asn1_time_to_time_t function in ext/openssl/openssl.c in PHP before 5.3.28, 5.4.x before 5.4.23, and 5.5.x before 5.5.7 does not properly parse (1) notBefore and (2) notAfter timestamps in X.509 certificates, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted certificate that is not properly handled by the openssl_x509_parse function.
CVE-2013-6424	Integer underflow in the xTrapezoidValid macro in render/picture.h in X.Org allows context-dependent attackers to cause a denial of service (crash) via a negative bottom value.
CVE-2013-6425	Integer underflow in the pixman_trapezoid_valid macro in pixman.h in Pixman before 0.32.0, as used in X.Org server and cairo, allows context-dependent attackers to cause a denial of service (crash) via a negative bottom value.
CVE-2013-6435	Race condition in RPM 4.11.1 and earlier allows remote attackers to execute arbitrary code via a crafted RPM file whose installation extracts the contents to temporary files before validating the signature, as demonstrated by installing a file in the /etc/cron.d directory.
CVE-2013-6438	The dav_xml_get_cdata function in main/util.c in the mod_dav module in the Apache HTTP Server before 2.4.8 does not properly remove whitespace characters from CDATA sections, which allows remote attackers to cause a denial of service (daemon crash) via a crafted DAV WRITE request.
CVE-2013-6449	The ssl_get_algorithm2 function in ssl/s3_lib.c in OpenSSL before 1.0.2 obtains a certain version number from an incorrect data structure, which allows remote attackers to cause a denial of service (daemon crash) via crafted traffic from a TLS 1.2 client.
CVE-2013-6450	The DTLS retransmission implementation in OpenSSL 1.0.0 before 1.0.0l and 1.0.1 before 1.0.1f does not properly maintain data structures for digest and

	encryption contexts, which might allow man-in-the-middle attackers to trigger the use of a different context and cause a denial of service (application crash) by interfering with packet delivery, related to ssl/d1_both.c and ssl/t1_enc.c.
CVE-2013-6462	Stack-based buffer overflow in the bdfReadCharacters function in bitmap/bdfread.c in X.Org libXfont 1.1 through 1.4.6 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string in a character name in a BDF font file.
CVE-2013-6466	Openswan 2.6.39 and earlier allows remote attackers to cause a denial of service (NULL pointer dereference and IKE daemon restart) via IKEv2 packets that lack expected payloads.
CVE-2013-6497	clamscan in ClamAV before 0.98.5, when using -a option, allows remote attackers to cause a denial of service (crash) as demonstrated by the jwplayer.js file.
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-2013-6712	The scan function in ext/date/lib/parse_iso_intervals.c in PHP through 5.5.6 does not properly restrict creation of DateInterval objects, which might allow remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted interval specification.
CVE-2013-6800	An unspecified third-party database module for the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) 1.10.x allows remote authenticated users to cause a denial of service (NULL pointer dereference

	and daemon crash) via a crafted request, a different vulnerability than CVE-2013-1418.
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-2013-7038	The MHD_http_unescape function in libmicrohttpd before 0.9.32 might allow remote attackers to obtain sensitive information or cause a denial of service (crash) via unspecified vectors that trigger an out-of-bounds read.
CVE-2013-7039	Stack-based buffer overflow in the MHD_digest_auth_check function in libmicrohttpd before 0.9.32, when MHD_OPTION_CONNECTION_MEMORY_LIMIT is set to a large value, allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long URI in an authentication header.
CVE-2013-7041	The pam_userdb module for Pam uses a case-insensitive method to compare hashed passwords, which makes it easier for attackers to guess the password via a brute force attack.
CVE-2013-7108	Multiple off-by-one errors in Nagios Core 3.5.1, 4.0.2, and earlier, and Icinga before 1.8.5, 1.9 before 1.9.4, and 1.10 before 1.10.2 allow remote authenticated users to obtain sensitive information from process memory or cause a denial of service (crash) via a long string in the last key value in the variable list to the process_cgivars function in (1) avail.c, (2) cmd.c, (3) config.c, (4) extinfo.c, (5) histogram.c, (6) notifications.c, (7) outages.c, (8) status.c, (9) statusmap.c, (10) summary.c, and (11) trends.c in cgi/, which triggers a heap-based buffer over-read.
CVE-2013-7112	The dissect_sip_common function in epan/dissectors/packet-sip.c in the SIP dissector in Wireshark 1.8.x before 1.8.12 and 1.10.x before 1.10.4 does not check for empty lines, which allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.
CVE-2013-7114	Multiple buffer overflows in the create_ntlmssp_v2_key function in epan/dissectors/packet-ntlmssp.c in the NTLMSSP v2 dissector in Wireshark 1.8.x before 1.8.12 and 1.10.x before 1.10.4 allow remote attackers to cause a denial of service (application crash) via a long domain name in a packet.

CVE-2013-7205	Off-by-one error in the process_cgivars function in contrib/daemonchk.c in Nagios Core 3.5.1, 4.0.2, and earlier allows remote authenticated users to obtain sensitive information from process memory or cause a denial of service (crash) via a long string in the last key value in the variable list, which triggers a heap-based buffer over-read.
CVE-2013-7226	Integer overflow in the gdImageCrop function in ext/gd/gd.c in PHP 5.5.x before 5.5.9 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an imagecrop function call with a large x dimension value, leading to a heap-based buffer overflow.
CVE-2013-7263	The Linux kernel before 3.12.4 updates certain length values before ensuring that associated data structures have been initialized, which allows local users to obtain sensitive information from kernel stack memory via a (1) recvfrom, (2) recvmmsg, or (3) recvmsg system call, related to net/ipv4/ping.c, net/ipv4/raw.c, net/ipv4/udp.c, net/ipv6/raw.c, and net/ipv6/udp.c.
CVE-2013-7265	The pn_recvmsg function in net/phonet/datagram.c in the Linux kernel before 3.12.4 updates a certain length value before ensuring that an associated data structure has been initialized, which allows local users to obtain sensitive information from kernel stack memory via a (1) recvfrom, (2) recvmmsg, or (3) recvmsg system call.
CVE-2013-7327	The gdImageCrop function in ext/gd/gd.c in PHP 5.5.x before 5.5.9 does not check return values, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via invalid imagecrop arguments that lead to use of a NULL pointer as a return value, a different vulnerability than CVE-2013-7226.
CVE-2013-7345	The BEGIN regular expression in the awk script detector in magic/Magdir/commands in file before 5.15 uses multiple wildcards with unlimited repetitions, which allows context-dependent attackers to cause a denial of service (CPU consumption) via a crafted ASCII file that triggers a large amount of backtracking, as demonstrated via a file with many newline characters.
CVE-2013-7423	The send_dg function in resolv/res_send.c in GNU C Library (aka glibc or libc6) before 2.20 does not properly reuse file descriptors, which allows remote attackers to send DNS queries to unintended locations via a large number of requests that trigger a call to the getaddrinfo function.
CVE-2013-7456	gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.1.1, as used in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7, allows remote attackers to cause a denial of service (out-of-bounds

	read) or possibly have unspecified other impact via a crafted image that is mishandled by the imagescale function.
CVE-2013-7459	Heap-based buffer overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to execute arbitrary code as demonstrated by a crafted iv parameter to cryptmsg.py.
CVE-2014-0001	Buffer overflow in client/mysql.cc in Oracle MySQL and MariaDB before 5.5.35 allows remote database servers to cause a denial of service (crash) and possibly execute arbitrary code via a long server version string.
CVE-2014-0011	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-0015	cURL and libcurl 7.10.6 through 7.34.0, when more than one authentication method is enabled, re-uses NTLM connections, which might allow context-dependent attackers to authenticate as other users via a request.
CVE-2014-0019	Stack-based buffer overflow in socat 1.3.0.0 through 1.7.2.2 and 2.0.0-b1 through 2.0.0-b6 allows local users to cause a denial of service (segmentation fault) via a long server name in the PROXY-CONNECT address in the command line.
CVE-2014-0021	[traffic amplification in cmdmon protocol]
CVE-2014-0022	The installUpdates function in yum-cron/yum-cron.py in yum 3.4.3 and earlier does not properly check the return value of the sigCheckPkg function, which allows remote attackers to bypass the RMP package signing restriction via an unsigned package.
CVE-2014-0032	The get_resource function in repos.c in the mod_dav_svn module in Apache Subversion before 1.7.15 and 1.8.x before 1.8.6, when SVNListParentPath is enabled, allows remote attackers to cause a denial of service (crash) via vectors related to the server root and request methods other than GET, as demonstrated by the "svn ls http://svn.example.com" command.
CVE-2014-0039	Untrusted search path vulnerability in fwsnort before 1.6.4, when not running as root, allows local users to execute arbitrary code via a Trojan horse fwsnort.conf in the current working directory.
CVE-2014-0050	MultipartStream.java in Apache Commons FileUpload before 1.3.1, as used in Apache Tomcat, JBoss Web, and other products, allows remote attackers to cause a denial of service (infinite loop and CPU consumption)

	via a crafted Content-Type header that bypasses a loop's intended exit conditions.
CVE-2014-0055	The get_rx_bufs function in drivers/vhost/net.c in the vhost-net subsystem in the Linux kernel package before 2.6.32-431.11.2 on Red Hat Enterprise Linux (RHEL) 6 does not properly handle vhost_get_vq_desc errors, which allows guest OS users to cause a denial of service (host OS crash) via unspecified vectors.
CVE-2014-0060	PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 does not properly enforce the ADMIN OPTION restriction, which allows remote authenticated members of a role to add or remove arbitrary users to that role by calling the SET ROLE command before the associated GRANT command.
CVE-2014-0061	The validator functions for the procedural languages (PLs) in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allow remote authenticated users to gain privileges via a function that is (1) defined in another language or (2) not allowed to be directly called by the user due to permissions.
CVE-2014-0062	Race condition in the (1) CREATE INDEX and (2) unspecified ALTER TABLE commands in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allows remote authenticated users to create an unauthorized index or read portions of unauthorized tables by creating or deleting a table with the same name during the timing window.
CVE-2014-0063	Multiple stack-based buffer overflows in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allow remote authenticated users to cause a denial of service (crash) or possibly execute arbitrary code via vectors related to an incorrect MAXDATELEN constant and datetime values involving (1) intervals, (2) timestamps, or (3) timezones, a different vulnerability than CVE-2014-0065.
CVE-2014-0064	Multiple integer overflows in the path_in and other unspecified functions in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allow remote authenticated users to have unspecified impact and attack vectors, which trigger a buffer overflow. NOTE: this identifier has been SPLIT due to different affected versions; use CVE-2014-2669 for the hstore vector.
CVE-2014-0065	Multiple buffer overflows in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 allow remote authenticated

	users to have unspecified impact and attack vectors, a different vulnerability than CVE-2014-0063.
CVE-2014-0066	The chkpass extension in PostgreSQL before 8.4.20, 9.0.x before 9.0.16, 9.1.x before 9.1.12, 9.2.x before 9.2.7, and 9.3.x before 9.3.3 does not properly check the return value of the crypt library function, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and crash) via unspecified vectors.
CVE-2014-0067	The "make check" command for the test suites in PostgreSQL 9.3.3 and earlier does not properly invoke initdb to specify the authentication requirements for a database cluster to be used for the tests, which allows local users to gain privileges by leveraging access to this cluster.
CVE-2014-0069	The cifs_iovec_write function in fs/cifs/file.c in the Linux kernel through 3.13.5 does not properly handle uncached write operations that copy fewer than the requested number of bytes, which allows local users to obtain sensitive information from kernel memory, cause a denial of service (memory corruption and system crash), or possibly gain privileges via a writev system call with a crafted pointer.
CVE-2014-0075	Integer overflow in the parseChunkHeader function in java/org/apache/coyote/http11/filters/ChunkedInputFilter.java in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4 allows remote attackers to cause a denial of service (resource consumption) via a malformed chunk size in chunked transfer coding of a request during the streaming of data.
CVE-2014-0077	drivers/vhost/net.c in the Linux kernel before 3.13.10, when mergeable buffers are disabled, does not properly validate packet lengths, which allows guest OS users to cause a denial of service (memory corruption and host OS crash) or possibly gain privileges on the host OS via crafted packets, related to the handle_rx and get_rx_bufs functions.
CVE-2014-0092	lib/x509/verify.c in GnuTLS before 3.1.22 and 3.2.x before 3.2.12 does not properly handle unspecified errors when verifying X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers via a crafted certificate.
CVE-2014-0096	java/org/apache/catalina/servlets/DefaultServlet.java in the default servlet in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4 does not properly restrict XSLT stylesheets, which allows remote attackers to bypass security-manager restrictions and read arbitrary files via a crafted web application that provides an XML external entity declaration in

	conjunction with an entity reference, related to an XML External Entity (XXE) issue.
CVE-2014-0098	The log_cookie function in mod_log_config.c in the mod_log_config module in the Apache HTTP Server before 2.4.8 allows remote attackers to cause a denial of service (segmentation fault and daemon crash) via a crafted cookie that is not properly handled during truncation.
CVE-2014-0099	Integer overflow in java/org/apache/tomcat/util/buf/Ascii.java in Apache Tomcat before 6.0.40, 7.x before 7.0.53, and 8.x before 8.0.4, when operated behind a reverse proxy, allows remote attackers to conduct HTTP request smuggling attacks via a crafted Content-Length HTTP header.
CVE-2014-0101	The sctp_sf_do_5_1D_ce function in net/sctp/sm_statefuns.c in the Linux kernel through 3.13.6 does not validate certain auth_enable and auth_capable fields before making an sctp_sf_authenticate call, which allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via an SCTP handshake with a modified INIT chunk and a crafted AUTH chunk before a COOKIE_ECHO chunk.
CVE-2014-0107	The TransformerFactory in Apache Xalan-Java before 2.7.2 does not properly restrict access to certain properties when FEATURE_SECURE_PROCESSING is enabled, which allows remote attackers to bypass expected restrictions and load arbitrary classes or access external resources via a crafted (1) xalan:content-header, (2) xalan:entities, (3) xslt:content-header, or (4) xslt:entities property, or a Java property that is bound to the XSLT 1.0 system-property function.
CVE-2014-0118	The deflate_in_filter function in mod_deflate.c in the mod_deflate module in the Apache HTTP Server before 2.4.10, when request body decompression is enabled, allows remote attackers to cause a denial of service (resource consumption) via crafted request data that decompresses to a much larger size.
CVE-2014-0128	Squid 3.1 before 3.3.12 and 3.4 before 3.4.4, when SSL-Bump is enabled, allows remote attackers to cause a denial of service (assertion failure) via a crafted range request, related to state management.
CVE-2014-0132	The SASL authentication functionality in 389 Directory Server before 1.2.11.26 allows remote authenticated users to connect as an arbitrary user and gain privileges via the authzid parameter in a SASL/GSSAPI bind.
CVE-2014-0133	Heap-based buffer overflow in the SPDY implementation in nginx 1.3.15 before 1.4.7 and 1.5.x before 1.5.12 allows remote attackers to execute arbitrary code via a crafted request.

CVE-2014-0138	The default configuration in cURL and libcurl 7.10.6 before 7.36.0 re-uses (1) SCP, (2) SFTP, (3) POP3, (4) POP3S, (5) IMAP, (6) IMAPS, (7) SMTP, (8) SMTPS, (9) LDAP, and (10) LDAPS connections, which might allow context-dependent attackers to connect as other users via a request, a similar issue to CVE-2014-0015.
CVE-2014-0160	The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.
CVE-2014-0172	Integer overflow in the check_section function in dwarf_begin_elf.c in the libdw library, as used in elfutils 0.153 and possibly through 0.158 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a malformed compressed debug section in an ELF file, which triggers a heap-based buffer overflow.
CVE-2014-0191	The xmlParserHandlePEReference function in parser.c in libxml2 before 2.9.2, as used in Web Listener in Oracle HTTP Server in Oracle Fusion Middleware 11.1.1.7.0, 12.1.2.0, and 12.1.3.0 and other products, loads external parameter entities regardless of whether entity substitution or validation is enabled, which allows remote attackers to cause a denial of service (resource consumption) via a crafted XML document.
CVE-2014-0195	The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.
CVE-2014-0196	The n_tty_write function in drivers/tty/n_tty.c in the Linux kernel through 3.14.3 does not properly manage tty driver access in the "LECHO & !OPOST" case, which allows local users to cause a denial of service (memory corruption and system crash) or gain privileges by triggering a race condition involving read and write operations with long strings.
CVE-2014-0198	The do_ssl3_write function in s3_pkt.c in OpenSSL 1.x through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, does not properly manage a buffer pointer during certain recursive calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors that trigger an alert condition.

CVE-2014-0206	Array index error in the aio_read_events_ring function in fs/aio.c in the Linux kernel through 3.15.1 allows local users to obtain sensitive information from kernel memory via a large head value.
CVE-2014-0207	The cdf_read_short_sector function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted CDF file.
CVE-2014-0209	Multiple integer overflows in the (1) FontFileAddEntry and (2) lexAlias functions in X.Org libXfont before 1.4.8 and 1.4.9x before 1.4.99.901 might allow local users to gain privileges by adding a directory with a large fonts.dir or fonts.alias file to the font path, which triggers a heap-based buffer overflow, related to metadata.
CVE-2014-0210	Multiple buffer overflows in X.Org libXfont before 1.4.8 and 1.4.9x before 1.4.99.901 allow remote font servers to execute arbitrary code via a crafted xfs protocol reply to the (1) _fs_recv_conn_setup, (2) fs_read_open_font, (3) fs_read_query_info, (4) fs_read_extent_info, (5) fs_read_glyphs, (6) fs_read_list, or (7) fs_read_list_info function.
CVE-2014-0211	Multiple integer overflows in the (1) fs_get_reply, (2) fs_alloc_glyphs, and (3) fs_read_extent_info functions in X.Org libXfont before 1.4.8 and 1.4.9x before 1.4.99.901 allow remote font servers to execute arbitrary code via a crafted xfs reply, which triggers a buffer overflow.
CVE-2014-0221	The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.
CVE-2014-0224	OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.
CVE-2014-0226	Race condition in the mod_status module in the Apache HTTP Server before 2.4.10 allows remote attackers to cause a denial of service (heap-based buffer overflow), or possibly obtain sensitive credential information or execute arbitrary code, via a crafted request that triggers improper scoreboard handling within the status_handler function in modules/generators/mod_status.c and the lua_ap_scoreboard_worker function in modules/lua/lua_request.c.

CVE-2014-0227	java/org/apache/coyote/http11/filters/ ChunkedInputFilter.java in Apache Tomcat 6.x before 6.0.42, 7.x before 7.0.55, and 8.x before 8.0.9 does not properly handle attempts to continue reading data after an error has occurred, which allows remote attackers to conduct HTTP request smuggling attacks or cause a denial of service (resource consumption) by streaming data with malformed chunked transfer coding.
CVE-2014-0230	Apache Tomcat 6.x before 6.0.44, 7.x before 7.0.55, and 8.x before 8.0.9 does not properly handle cases where an HTTP response occurs before finishing the reading of an entire request body, which allows remote attackers to cause a denial of service (thread consumption) via a series of aborted upload attempts.
CVE-2014-0231	The mod_cgid module in the Apache HTTP Server before 2.4.10 does not have a timeout mechanism, which allows remote attackers to cause a denial of service (process hang) via a request to a CGI script that does not read from its stdin file descriptor.
CVE-2014-0237	The cdf_unpack_summary_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (performance degradation) by triggering many file_printf calls.
CVE-2014-0238	The cdf_read_property_info function in cdf.c in the Fileinfo component in PHP before 5.4.29 and 5.5.x before 5.5.13 allows remote attackers to cause a denial of service (infinite loop or out-of-bounds memory access) via a vector that (1) has zero length or (2) is too long.
CVE-2014-0240	The mod_wsgi module before 3.5 for Apache, when daemon mode is enabled, does not properly handle error codes returned by setuid when run on certain Linux kernels, which allows local users to gain privileges via vectors related to the number of running processes.
CVE-2014-0242	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-0368	Unspecified vulnerability in Oracle Java SE 5.0u55, 6u65, and 7u45, and Java SE Embedded 7u45, allows remote attackers to affect confidentiality via unknown vectors related to Networking. NOTE: the previous information is from the January 2014 CPU. Oracle has not commented on third-party claims that the issue is related to incorrect permission checks when listening

	on a socket, which allows attackers to escape the sandbox.
CVE-2014-0373	Unspecified vulnerability in Oracle Java SE 5.0u55, 6u65, and 7u45, and OpenJDK 7, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Serviceability. NOTE: the previous information is from the January 2014 CPU. Oracle has not commented on third-party claims that the issue is related to throwing of an incorrect exception when SnmpStatusException should have been used in the SNMP implementation, which allows attackers to escape the sandbox.
CVE-2014-0376	Unspecified vulnerability in Oracle Java SE 5.0u55, 6u65, and 7u45; Java SE Embedded 7u45; and OpenJDK 7 allows remote attackers to affect integrity via vectors related to JAXP. NOTE: the previous information is from the January 2014 CPU. Oracle has not commented on third-party claims that the issue is related to an improper check for "code permissions when creating document builder factories."
CVE-2014-0384	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.5.35 and earlier and 5.6.15 and earlier allows remote authenticated users to affect availability via vectors related to XML.
CVE-2014-0386	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.71 and earlier, 5.5.33 and earlier, and 5.6.13 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.
CVE-2014-0393	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.71 and earlier, 5.5.33 and earlier, and 5.6.13 and earlier allows remote authenticated users to affect integrity via unknown vectors related to InnoDB.
CVE-2014-0401	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.72 and earlier, 5.5.34 and earlier, and 5.6.14 and earlier allows remote authenticated users to affect availability via unknown vectors.
CVE-2014-0402	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.71 and earlier, 5.5.33 and earlier, and 5.6.13 and earlier allows remote authenticated users to affect availability via unknown vectors related to Locking.
CVE-2014-0411	Unspecified vulnerability in Oracle Java SE 5.0u55, 6u65, and 7u45; JRockit R27.7.7 and R28.2.9; Java SE Embedded 7u45; and OpenJDK 7 allows remote attackers to affect confidentiality and integrity via vectors related to JSSE. NOTE: the previous information is from the January 2014 CPU. Oracle has

	not commented on third-party claims that this issue allows remote attackers to obtain sensitive information about encryption keys via a timing discrepancy during the TLS/SSL handshake.
CVE-2014-0412	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.72 and earlier, 5.5.34 and earlier, and 5.6.14 and earlier allows remote authenticated users to affect availability via unknown vectors related to InnoDB.
CVE-2014-0416	Unspecified vulnerability in Oracle Java SE 5.0u55, 6u65, and 7u45; Java SE Embedded 7u45; and OpenJDK 7 allows remote attackers to affect integrity via vectors related to JAAS. NOTE: the previous information is from the January 2014 CPU. Oracle has not commented on third-party claims that the issue is related to how principals are set for the Subject class, which allows attackers to escape the sandbox using deserialization of a crafted Subject instance.
CVE-2014-0422	Unspecified vulnerability in Oracle Java SE 5.0u55, 6u65, and 7u45; Java SE Embedded 7u45; and OpenJDK 7 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JNDI. NOTE: the previous information is from the January 2014 CPU. Oracle has not commented on third-party claims that the issue is related to missing package access checks in the Naming / JNDI component, which allows attackers to escape the sandbox.
CVE-2014-0423	Unspecified vulnerability in Oracle Java SE 5.0u55, 6u65, and 7u45; JRockit R27.7.7 and R28.2.9; Java SE Embedded 7u45; and OpenJDK 7 allows remote authenticated users to affect confidentiality and availability via unknown vectors related to Beans. NOTE: the previous information is from the January 2014 CPU. Oracle has not commented on third-party claims that this issue is an XML External Entity (XXE) vulnerability in DocumentHandler.java, related to Beans decoding.
CVE-2014-0428	Unspecified vulnerability in Oracle Java SE 5.0u55, 6u65, and 7u45; Java SE Embedded 7u45; and OpenJDK 7 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to CORBA. NOTE: the previous information is from the January 2014 CPU. Oracle has not commented on third-party claims that the issue is related to "insufficient security checks in IIOP streams," which allows attackers to escape the sandbox.
CVE-2014-0429	Unspecified vulnerability in Oracle Java SE 5.0u61, 6u71, 7u51, and 8; JRockit R27.8.1 and R28.3.1; and Java SE Embedded 7u51 allows remote attackers

	to affect confidentiality, integrity, and availability via unknown vectors related to 2D.
CVE-2014-0437	Unspecified vulnerability in the MySQL Server component in Oracle MySQL 5.1.72 and earlier, 5.5.34 and earlier, and 5.6.14 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.
CVE-2014-0446	Unspecified vulnerability in Oracle Java SE 5.0u61, 6u71, 7u51, and 8, and Java SE Embedded 7u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.
CVE-2014-0451	Unspecified vulnerability in Oracle Java SE 5.0u61, 6u71, 7u51, and 8, and Java SE Embedded 7u51, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to AWT, a different vulnerability than CVE-2014-2412.
CVE-2014-0452	Unspecified vulnerability in Oracle Java SE 6u71, 7u51, and 8, and Java SE Embedded 7u51, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JAX-WS, a different vulnerability than CVE-2014-0458 and CVE-2014-2423.
CVE-2014-0453	Unspecified vulnerability in Oracle Java SE 5.0u61, 6u71, 7u51, and 8; JRockit R27.8.1 and R28.3.1; and Java SE Embedded 7u51 allows remote attackers to affect confidentiality and integrity via unknown vectors related to Security.
CVE-2014-0454	Unspecified vulnerability in Oracle Java SE 7u51 and 8, and Java SE Embedded 7u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Security.
CVE-2014-0455	Unspecified vulnerability in Oracle Java SE 7u51 and 8, and Java SE Embedded 7u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2014-0432 and CVE-2014-2402.
CVE-2014-0456	Unspecified vulnerability in Oracle Java SE 6u71, 7u51, and 8, and Java SE Embedded 7u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot.
CVE-2014-0457	Unspecified vulnerability in Oracle Java SE 5.0u61, SE 6u71, 7u51, and 8; JRockit R27.8.1 and R28.3.1; and Java SE Embedded 7u51 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.
CVE-2014-0458	Unspecified vulnerability in Oracle Java SE 6u71, 7u51, and 8, and Java SE Embedded 7u51, allows remote attackers to affect confidentiality, integrity, and

	availability via vectors related to JAX-WS, a different vulnerability than CVE-2014-0452 and CVE-2014-2423.
CVE-2014-0459	Unspecified vulnerability in Oracle Java SE 7u51 and 8, and Java SE Embedded 7u51, allows remote attackers to affect availability via unknown vectors related to 2D.
CVE-2014-0460	Unspecified vulnerability in Oracle Java SE 5.0u61, 6u71, 7u51, and 8; JRockit R27.8.1 and R28.3.1; and Java SE Embedded 7u51 allows remote attackers to affect confidentiality and integrity via vectors related to JNDI.
CVE-2014-0461	Unspecified vulnerability in Oracle Java SE 6u71, 7u51, and 8, and Java SE Embedded 7u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.
CVE-2014-0467	Buffer overflow in copy.c in Mutt before 1.5.23 allows remote attackers to cause a denial of service (crash) via a crafted RFC2047 header line, related to address expansion.
CVE-2014-0475	Multiple directory traversal vulnerabilities in GNU C Library (aka glibc or libc6) before 2.20 allow context-dependent attackers to bypass ForceCommand restrictions and possibly have other unspecified impact via a .. (dot dot) in a (1) LC_*, (2) LANG, or other locale environment variable.
CVE-2014-0476	The slapper function in chkrootkit before 0.50 does not properly quote file paths, which allows local users to execute arbitrary code via a Trojan horse executable. NOTE: this is only a vulnerability when /tmp is not mounted with the noexec option.
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-2014-0591	The query_findclosestnsec3 function in query.c in named in ISC BIND 9.6, 9.7, and 9.8 before 9.8.6-P2 and 9.9 before 9.9.4-P2, and 9.6-ESV before 9.6-ESV-R10-P2, allows remote attackers to cause a denial of service (INSIST assertion failure and daemon exit) via a crafted DNS query to an authoritative nameserver that uses the NSEC3 signing feature.
CVE-2014-0978	Stack-based buffer overflow in the yyerror function in lib/cgraph/scan.l in Graphviz 2.34.0 allows remote attackers to have unspecified impact via a long line in a dot file.
CVE-2014-1235	Stack-based buffer overflow in the "yyerror" function in Graphviz 2.34.0 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted file. NOTE: This vulnerability exists due to an incomplete fix for CVE-2014-0978.
CVE-2014-1236	Stack-based buffer overflow in the chkNum function in lib/cgraph/scan.l in Graphviz 2.34.0 allows remote attackers to have unspecified impact via vectors related to a "badly formed number" and a "long digit list."
CVE-2014-1402	The default configuration for bccache.FileSystemBytecodeCache in Jinja2 before 2.7.2 does not properly create temporary files, which allows local users to gain privileges via a crafted .cache file with a name starting with __jinja2_ in /tmp.
CVE-2014-1492	The cert_TestHostName function in lib/certdb/certdb.c in the certificate-checking implementation in Mozilla Network Security Services (NSS) before 3.16 accepts a wildcard character that is embedded in an internationalized domain name's U-label, which might allow man-in-the-middle attackers to spoof SSL servers via a crafted certificate.
CVE-2014-1544	Use-after-free vulnerability in the CERT_DestroyCertificate function in libnss3.so in Mozilla Network Security Services (NSS) 3.x, as used in Firefox before 31.0, Firefox ESR 24.x before 24.7, and Thunderbird before 24.7, allows remote attackers to execute arbitrary code via vectors that trigger certain improper removal of an NSSCertificate structure from a trust domain.
CVE-2014-1545	Mozilla Netscape Portable Runtime (NSPR) before 4.10.6 allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds write) via vectors involving the sprintf and console functions.
CVE-2014-1568	Mozilla Network Security Services (NSS) before 3.16.2.1, 3.16.x before 3.16.5, and 3.17.x before 3.17.1, as used in Mozilla Firefox before 32.0.3, Mozilla Firefox ESR 24.x before 24.8.1 and 31.x before 31.1.1, Mozilla Thunderbird before 24.8.1 and 31.x before 31.1.2, Mozilla SeaMonkey before 2.29.1, Google

	Chrome before 37.0.2062.124 on Windows and OS X, and Google Chrome OS before 37.0.2062.120, does not properly parse ASN.1 values in X.509 certificates, which makes it easier for remote attackers to spoof RSA signatures via a crafted certificate, aka a "signature malleability" issue.
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-2014-1739	The media_device_enum_entities function in drivers/media/media-device.c in the Linux kernel before 3.14.6 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel memory by leveraging /dev/media0 read access for a MEDIA_IOC_ENUM_ENTITIES ioctl call.
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-2014-1858	Insecure temporary file use in __init__.py
CVE-2014-1859	Insecure temporary file uses
CVE-2014-1874	The security_context_to_sid_core function in security/selinux/ss/services.c in the Linux kernel before 3.13.4 allows local users to cause a denial of service (system crash) by leveraging the CAP_MAC_ADMIN capability to set a zero-length security context.
CVE-2014-1875	The Capture::Tiny module before 0.24 for Perl allows local users to write to arbitrary files via a symlink attack on a temporary file.
CVE-2014-1876	The unpacker::redirect_stdio function in unpack.cpp in unpack200 in OpenJDK 6, 7, and 8; Oracle Java SE 5.0u61, 6u71, 7u51, and 8; JRockit R27.8.1 and R28.3.1; and Java SE Embedded 7u51 does not securely create temporary files when a log file cannot be opened, which allows local users to overwrite arbitrary files via a symlink attack on /tmp/unpack.log.
CVE-2014-1878	Stack-based buffer overflow in the cmd_submitf function in cgi/cmd.c in Nagios Core, possibly 4.0.3rc1 and earlier, and Icinga before 1.8.6, 1.9 before 1.9.5, and 1.10 before 1.10.3 allows remote attackers to cause a denial of service (segmentation fault) via a long message to cmd.cgi.

CVE-2014-1912	Buffer overflow in the socket.recvfrom_into function in Modules/socketmodule.c in Python 2.5 before 2.7.7, 3.x before 3.3.4, and 3.4.x before 3.4rc1 allows remote attackers to execute arbitrary code via a crafted string.
CVE-2014-1943	Fine Free file before 5.17 allows context-dependent attackers to cause a denial of service (infinite recursion, CPU consumption, and crash) via a crafted indirect offset value in the magic of a file.
CVE-2014-1947	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-1958	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-2015	Stack-based buffer overflow in the normify function in the rlm_pap module (modules/rlm_pap/rlm_pap.c) in FreeRADIUS 2.x, possibly 2.2.3 and earlier, and 3.x, possibly 3.0.1 and earlier, might allow attackers to cause a denial of service (crash) and possibly execute arbitrary code via a long password hash, as demonstrated by an SSHA hash.
CVE-2014-2030	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-2270	softmagic.c in file before 5.17 and libmagic allows context-dependent attackers to cause a denial of service (out-of-bounds memory access and crash) via crafted offsets in the softmagic of a PE executable.
CVE-2014-2277	insecure temporary file usage
CVE-2014-2281	The nfs_name_snoop_add_name function in epan/dissectors/packet-nfs.c in the NFS dissector in Wireshark 1.8.x before 1.8.13 and 1.10.x before 1.10.6 does not validate a certain length value, which allows remote attackers to cause a denial of service (memory corruption and application crash) via a crafted NFS packet.
CVE-2014-2283	epan/dissectors/packet-rlc in the RLC dissector in Wireshark 1.8.x before 1.8.13 and 1.10.x before 1.10.6 uses inconsistent memory-management approaches, which allows remote attackers to cause a denial of

	service (use-after-free error and application crash) via a crafted UMTS Radio Link Control packet.
CVE-2014-2284	The Linux implementation of the ICMP-MIB in Net-SNMP 5.5 before 5.5.2.1, 5.6.x before 5.6.2.1, and 5.7.x before 5.7.2.1 does not properly validate input, which allows remote attackers to cause a denial of service via unspecified vectors.
CVE-2014-2299	Buffer overflow in the mpeg_read function in wiretap/mpeg.c in the MPEG parser in Wireshark 1.8.x before 1.8.13 and 1.10.x before 1.10.6 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a large record in MPEG data.
CVE-2014-2309	The ip6_route_add function in net/ipv6/route.c in the Linux kernel through 3.13.6 does not properly count the addition of routes, which allows remote attackers to cause a denial of service (memory consumption) via a flood of ICMPv6 Router Advertisement packets.
CVE-2014-2323	SQL injection vulnerability in mod_mysql_vhost.c in lighttpd before 1.4.35 allows remote attackers to execute arbitrary SQL commands via the host name, related to request_check_hostname.
CVE-2014-2324	Multiple directory traversal vulnerabilities in (1) mod_evhost and (2) mod_simple_vhost in lighttpd before 1.4.35 allow remote attackers to read arbitrary files via a .. (dot dot) in the host name, related to request_check_hostname.
CVE-2014-2326	Cross-site scripting (XSS) vulnerability in cdef.php in Cacti 0.8.7g, 0.8.8b, and earlier allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2014-2327	Cross-site request forgery (CSRF) vulnerability in Cacti 0.8.7g, 0.8.8b, and earlier allows remote attackers to hijack the authentication of users for unspecified commands, as demonstrated by requests that (1) modify binary files, (2) modify configurations, or (3) add arbitrary users.
CVE-2014-2328	lib/graph_export.php in Cacti 0.8.7g, 0.8.8b, and earlier allows remote authenticated users to execute arbitrary commands via shell metacharacters in unspecified vectors.
CVE-2014-2397	Unspecified vulnerability in Oracle Java SE 7u51 and 8, and Java SE Embedded 7u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot.
CVE-2014-2398	Unspecified vulnerability in Oracle Java SE 5.0u61, 6u71, 7u51, and 8; JavaFX 2.2.51; and JRockit R27.8.1 and R28.3.1 allows remote authenticated users to affect integrity via unknown vectors related to Javadoc.

CVE-2014-2402	Unspecified vulnerability in Oracle Java SE 7u51 and 8, and Java SE Embedded 7u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2014-0432 and CVE-2014-0455.
CVE-2014-2403	Unspecified vulnerability in Oracle Java SE 6u71, 7u51, and 8, and Java SE Embedded 7u51, allows remote attackers to affect confidentiality via vectors related to JAXP.
CVE-2014-2412	Unspecified vulnerability in Oracle Java SE 5.0u61, 6u71, SE 7u51, and 8, and Java SE Embedded 7u51, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to AWT, a different vulnerability than CVE-2014-0451.
CVE-2014-2413	Unspecified vulnerability in Oracle Java SE 7u51 and 8, and Java SE Embedded 7u51, allows remote attackers to affect integrity via unknown vectors related to Libraries.
CVE-2014-2414	Unspecified vulnerability in Oracle Java SE 6u71, 7u51, and 8, and Java SE Embedded 7u51, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JAXB.
CVE-2014-2419	Unspecified vulnerability in Oracle MySQL Server 5.5.35 and earlier and 5.6.15 and earlier allows remote authenticated users to affect availability via unknown vectors related to Partition.
CVE-2014-2421	Unspecified vulnerability in Oracle Java SE 5.0u61, 6u71, 7u51, and 8; JavaFX 2.2.51; and Java SE Embedded 7u51 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.
CVE-2014-2423	Unspecified vulnerability in Oracle Java SE 6u71, 7u51, and 8, and Java SE Embedded 7u51, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JAX-WS, a different vulnerability than CVE-2014-0452 and CVE-2014-0458.
CVE-2014-2427	Unspecified vulnerability in Oracle Java SE 5.0u61, 6u71, 7u51, and 8, and Java SE Embedded 7u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Sound.
CVE-2014-2430	Unspecified vulnerability in Oracle MySQL Server 5.5.36 and earlier and 5.6.16 and earlier allows remote authenticated users to affect availability via unknown vectors related to Performance Schema.
CVE-2014-2431	Unspecified vulnerability in Oracle MySQL Server 5.5.36 and earlier and 5.6.16 and earlier allows remote attackers to affect availability via unknown vectors related to Options.

CVE-2014-2432	Unspecified vulnerability Oracle the MySQL Server component 5.5.35 and earlier and 5.6.15 and earlier allows remote authenticated users to affect availability via unknown vectors related to Federated.
CVE-2014-2436	Unspecified vulnerability in Oracle MySQL Server 5.5.36 and earlier and 5.6.16 and earlier allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to RBR.
CVE-2014-2438	Unspecified vulnerability in Oracle MySQL Server 5.5.35 and earlier and 5.6.15 and earlier allows remote authenticated users to affect availability via unknown vectors related to Replication.
CVE-2014-2440	Unspecified vulnerability in the MySQL Client component in Oracle MySQL 5.5.36 and earlier and 5.6.16 and earlier allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.
CVE-2014-2483	Unspecified vulnerability in the Java SE component in Oracle Java SE Java SE 7u60 and OpenJDK 7 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2014-4223. NOTE: the previous information is from the July 2014 CPU. Oracle has not commented on another vendor's claim that the issue is related to improper restriction of the "use of privileged annotations."
CVE-2014-2490	Unspecified vulnerability in the Java SE component in Oracle Java SE 7u60 and SE 8u5 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot.
CVE-2014-2497	The gdImageCreateFromXpm function in gdxpm.c in libgd, as used in PHP 5.4.26 and earlier, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted color table in an XPM file.
CVE-2014-2523	net/netfilter/nf_conntrack_proto_dccp.c in the Linux kernel through 3.13.6 uses a DCCP header pointer incorrectly, which allows remote attackers to cause a denial of service (system crash) or possibly execute arbitrary code via a DCCP packet that triggers a call to the (1) dccp_new, (2) dccp_packet, or (3) dccp_error function.
CVE-2014-2524	The _rl_tropen function in util.c in GNU readline before 6.3 patch 3 allows local users to create or overwrite arbitrary files via a symlink attack on a /var/tmp/rltrace.[PID] file.
CVE-2014-2525	Heap-based buffer overflow in the yaml_parser_scan_uri_escapes function in LibYAML before 0.1.6 allows context-dependent attackers to

	execute arbitrary code via a long sequence of percent-encoded characters in a URI in a YAML file.
CVE-2014-2532	sshd in OpenSSH before 6.6 does not properly support wildcards on AcceptEnv lines in sshd_config, which allows remote attackers to bypass intended environment restrictions by using a substring located before a wildcard character.
CVE-2014-2583	Multiple directory traversal vulnerabilities in pam_timestamp.c in the pam_timestamp module for Linux-PAM (aka pam) 1.1.8 allow local users to create arbitrary files or possibly bypass authentication via a .. (dot dot) in the (1) PAM_RUSER value to the get_ruser function or (2) PAM_TTY value to the check_tty function, which is used by the format_timestamp_name function.
CVE-2014-2653	The verify_host_key function in sshconnect.c in the client in OpenSSH 6.6 and earlier allows remote servers to trigger the skipping of SSHFP DNS RR checking by presenting an unacceptable HostCertificate.
CVE-2014-2681	Zend Framework 1 (ZF1) before 1.12.4, Zend Framework 2 before 2.1.6 and 2.2.x before 2.2.6, ZendOpenId, ZendRest, ZendService_AudioScrobbler, ZendService_Nirvanix, ZendService_SlideShare, ZendService_Technorati, and ZendService_WindowsAzure before 2.0.2, ZendService_Amazon before 2.0.3, and ZendService_Api before 1.0.0 allow remote attackers to read arbitrary files, send HTTP requests to intranet servers, and possibly cause a denial of service (CPU and memory consumption) via an XML External Entity (XXE) attack. NOTE: this issue exists because of an incomplete fix for CVE-2012-5657.
CVE-2014-2682	Zend Framework 1 (ZF1) before 1.12.4, Zend Framework 2 before 2.1.6 and 2.2.x before 2.2.6, ZendOpenId, ZendRest, ZendService_AudioScrobbler, ZendService_Nirvanix, ZendService_SlideShare, ZendService_Technorati, and ZendService_WindowsAzure before 2.0.2, ZendService_Amazon before 2.0.3, and ZendService_Api before 1.0.0, when PHP-FPM is used, does not properly share the libxml_disable_entity_loader setting between threads, which might allow remote attackers to conduct XML External Entity (XXE) attacks via an XML external entity declaration in conjunction with an entity reference. NOTE: this issue exists because of an incomplete fix for CVE-2012-5657.
CVE-2014-2683	Zend Framework 1 (ZF1) before 1.12.4, Zend Framework 2 before 2.1.6 and 2.2.x before 2.2.6, ZendOpenId, ZendRest,

	ZendService_AudioScrobbler, ZendService_Nirvanix, ZendService_SlideShare, ZendService_Technorati, and ZendService_WindowsAzure before 2.0.2, ZendService_Amazon before 2.0.3, and ZendService_Api before 1.0.0 allow remote attackers to cause a denial of service (CPU consumption) via (1) recursive or (2) circular references in an XML entity definition in an XML DOCTYPE declaration, aka an XML Entity Expansion (XEE) attack. NOTE: this issue exists because of an incomplete fix for CVE-2012-6532.
CVE-2014-2684	The GenericConsumer class in the Consumer component in ZendOpenId before 2.0.2 and the Zend_OpenId_Consumer class in Zend Framework 1 before 1.12.4 does not verify that the openid_op_endpoint value identifies the same Identity Provider as the provider used in the association handle, which allows remote attackers to bypass authentication and spoof arbitrary OpenID identities by using a malicious OpenID Provider that generates OpenID tokens with arbitrary identifier and claimed_id values.
CVE-2014-2685	The GenericConsumer class in the Consumer component in ZendOpenId before 2.0.2 and the Zend_OpenId_Consumer class in Zend Framework 1 before 1.12.4 violate the OpenID 2.0 protocol by ensuring only that at least one field is signed, which allows remote attackers to bypass authentication by leveraging an assertion from an OpenID provider.
CVE-2014-2708	Multiple SQL injection vulnerabilities in graph_xport.php in Cacti 0.8.7g, 0.8.8b, and earlier allow remote attackers to execute arbitrary SQL commands via the (1) graph_start, (2) graph_end, (3) graph_height, (4) graph_width, (5) graph_nolegend, (6) print_source, (7) local_graph_id, or (8) rra_id parameter.
CVE-2014-2709	lib/rrd.php in Cacti 0.8.7g, 0.8.8b, and earlier allows remote attackers to execute arbitrary commands via shell metacharacters in unspecified parameters.
CVE-2014-2856	Cross-site scripting (XSS) vulnerability in scheduler/client.c in Common Unix Printing System (CUPS) before 1.7.2 allows remote attackers to inject arbitrary web script or HTML via the URL path, related to the is_path_absolute function.
CVE-2014-2913	** DISPUTED ** Incomplete blacklist vulnerability in nrpe.c in Nagios Remote Plugin Executor (NRPE) 2.15 and earlier allows remote attackers to execute arbitrary commands via a newline character in the -a option to libexec/check_nrpe. NOTE: this issue is disputed by multiple parties. It has been reported that the vendor allows newlines as "expected behavior." Also, this issue can only occur when the administrator enables the "dont_blame_nrpe" option in nrpe.conf despite the "HIGH security risk" warning within the comments.

CVE-2014-2972	expand.c in Exim before 4.83 expands mathematical comparisons twice, which allows local users to gain privileges and execute arbitrary commands via a crafted lookup value.
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-2014-3153	The futex_requeue function in kernel/futex.c in the Linux kernel through 3.14.5 does not ensure that calls have two different futex addresses, which allows local users to gain privileges via a crafted FUTEX_REQUEUE command that facilitates unsafe waiter modification.
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-2014-3215	seunshare in policycoreutils 2.2.5 is owned by root with 4755 permissions, and executes programs in a way that changes the relationship between the setuid system call and the getresuid saved set-user-ID value, which makes it easier for local users to gain privileges by leveraging a program that mistakenly expected that it could permanently drop privileges.
CVE-2014-3248	Untrusted search path vulnerability in Puppet Enterprise 2.8 before 2.8.7, Puppet before 2.7.26 and 3.x before 3.6.2, Facter 1.6.x and 2.x before 2.0.2, Hiera before

	1.3.4, and Mcollective before 2.5.2, when running with Ruby 1.9.1 or earlier, allows local users to gain privileges via a Trojan horse file in the current working directory, as demonstrated using (1) rubygems/defaults/operating_system.rb, (2) Win32API.rb, (3) Win32API.so, (4) safe_yaml.rb, (5) safe_yaml/deep.rb, or (6) safe_yaml/deep.so; or (7) operatingsystem.rb, (8) operatingsystem.so, (9) osfamily.rb, or (10) osfamily.so in puppet/confine.
CVE-2014-3416	uPortal before 4.0.13.1 does not properly check the MANAGE permissions, which allows remote authenticated users to manage arbitrary portlets by leveraging the SUBSCRIBE permission for the portlet-admin portlet.
CVE-2014-3430	Dovecot 1.1 before 2.2.13 and dovecot-ee before 2.1.7.7 and 2.2.x before 2.2.12.12 does not properly close old connections, which allows remote attackers to cause a denial of service (resource consumption) via an incomplete SSL/TLS handshake for an IMAP/POP3 connection.
CVE-2014-3466	Buffer overflow in the read_server_hello function in lib/gnutls_handshake.c in GnuTLS before 3.1.25, 3.2.x before 3.2.15, and 3.3.x before 3.3.4 allows remote servers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a long session id in a ServerHello message.
CVE-2014-3467	Multiple unspecified vulnerabilities in the DER decoder in GNU Libtasn1 before 3.6, as used in GnuTLS, allow remote attackers to cause a denial of service (out-of-bounds read) via crafted ASN.1 data.
CVE-2014-3468	The asn1_get_bit_der function in GNU Libtasn1 before 3.6 does not properly report an error when a negative bit length is identified, which allows context-dependent attackers to cause out-of-bounds access via crafted ASN.1 data.
CVE-2014-3469	The (1) asn1_read_value_type and (2) asn1_read_value functions in GNU Libtasn1 before 3.6 allows context-dependent attackers to cause a denial of service (NULL pointer dereference and crash) via a NULL value in an ivalue argument.
CVE-2014-3470	The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.
CVE-2014-3478	Buffer overflow in the mconvert function in softmagic.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, allows remote attackers to cause a denial of service

	(application crash) via a crafted Pascal string in a FILE_PSTRING conversion.
CVE-2014-3479	The cdf_check_stream_offset function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, relies on incorrect sector-size data, which allows remote attackers to cause a denial of service (application crash) via a crafted stream offset in a CDF file.
CVE-2014-3480	The cdf_count_chain function in cdf.c in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, does not properly validate sector-count data, which allows remote attackers to cause a denial of service (application crash) via a crafted CDF file.
CVE-2014-3487	The cdf_read_property_info function in file before 5.19, as used in the Fileinfo component in PHP before 5.4.30 and 5.5.x before 5.5.14, does not properly validate a stream offset, which allows remote attackers to cause a denial of service (application crash) via a crafted CDF file.
CVE-2014-3504	The (1) serf_ssl_cert_issuer, (2) serf_ssl_cert_subject, and (3) serf_ssl_cert_certificate functions in Serf 0.2.0 through 1.3.x before 1.3.7 does not properly handle a NUL byte in a domain name in the subject's Common Name (CN) field of an X.509 certificate, which allows man-in-the-middle attackers to spoof arbitrary SSL servers via a crafted certificate issued by a legitimate Certification Authority.
CVE-2014-3505	Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.
CVE-2014-3506	d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.
CVE-2014-3507	Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.
CVE-2014-3508	The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters,

	which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.
CVE-2014-3509	Race condition in the ssl_parse_serverhello_tlsext function in t1_lib.c in OpenSSL 1.0.0 before 1.0.0n and 1.0.1 before 1.0.1i, when multithreading and session resumption are used, allows remote SSL servers to cause a denial of service (memory overwrite and client application crash) or possibly have unspecified other impact by sending Elliptic Curve (EC) Supported Point Formats Extension data.
CVE-2014-3510	The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.
CVE-2014-3511	The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 1.0.1 before 1.0.1i allows man-in-the-middle attackers to force the use of TLS 1.0 by triggering ClientHello message fragmentation in communication between a client and server that both support later TLS versions, related to a "protocol downgrade" issue.
CVE-2014-3512	Multiple buffer overflows in crypto/srp/srp_lib.c in the SRP implementation in OpenSSL 1.0.1 before 1.0.1i allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an invalid SRP (1) g, (2) A, or (3) B parameter.
CVE-2014-3513	Memory leak in d1_srtp.c in the DTLS SRTP extension in OpenSSL 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted handshake message.
CVE-2014-3515	The SPL component in PHP before 5.4.30 and 5.5.x before 5.5.14 incorrectly anticipates that certain data structures will have the array data type after unserialization, which allows remote attackers to execute arbitrary code via a crafted string that triggers use of a Hashtable destructor, related to "type confusion" issues in (1) ArrayObject and (2) SPLObjectStorage.
CVE-2014-3522	The Serf RA layer in Apache Subversion 1.4.0 through 1.7.x before 1.7.18 and 1.8.x before 1.8.10 does not properly handle wildcards in the Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof servers via a crafted certificate.

CVE-2014-3537	The web interface in CUPS before 1.7.4 allows local users in the lp group to read arbitrary files via a symlink attack on a file in /var/cache/cups/rss/.
CVE-2014-3538	file before 5.19 does not properly restrict the amount of data read during a regex search, which allows remote attackers to cause a denial of service (CPU consumption) via a crafted file that triggers backtracking during processing of an awk rule. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-7345.
CVE-2014-3562	Red Hat Directory Server 8 and 389 Directory Server, when debugging is enabled, allows remote attackers to obtain sensitive replicated metadata by searching the directory.
CVE-2014-3564	Multiple heap-based buffer overflows in the status_handler function in (1) engine-gpgsm.c and (2) engine-uiserver.c in GPGME before 1.5.1 allow remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to "different line lengths in a specific order."
CVE-2014-3566	The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.
CVE-2014-3567	Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.
CVE-2014-3568	OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.
CVE-2014-3569	The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 0.9.8zc, 1.0.0o, and 1.0.1j does not properly handle attempts to use unsupported protocols, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an unexpected handshake, as demonstrated by an SSLv3 handshake to a no-ssl3 application with certain error handling. NOTE: this issue became relevant after the CVE-2014-3568 fix.
CVE-2014-3570	The BN_sqr implementation in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not properly calculate the square of a BIGNUM value, which might make it easier for remote attackers to defeat cryptographic protection mechanisms via

	unspecified vectors, related to crypto/bn/asm/mips.pl, crypto/bn/asm/x86_64-gcc.c, and crypto/bn/bn_asm.c.
CVE-2014-3571	OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted DTLS message that is processed with a different read operation for the handshake header than for the handshake body, related to the dtls1_get_record function in d1_pkt.c and the ssl3_read_n function in s3_pkt.c.
CVE-2014-3572	The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct ECDHE-to-ECDH downgrade attacks and trigger a loss of forward secrecy by omitting the ServerKeyExchange message.
CVE-2014-3577	org.apache.http.conn.ssl.AbstractVerifier in Apache HttpComponents HttpClient before 4.3.5 and HttpAsyncClient before 4.0.2 does not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via a "CN=" string in a field in the distinguished name (DN) of a certificate, as demonstrated by the "foo,CN=www.apache.org" string in the O field.
CVE-2014-3580	The mod_dav_svn Apache HTTPD server module in Apache Subversion 1.x before 1.7.19 and 1.8.x before 1.8.11 allows remote attackers to cause a denial of service (NULL pointer dereference and server crash) via a REPORT request for a resource that does not exist.
CVE-2014-3581	The cache_merge_headers_out function in modules/cache/cache_util.c in the mod_cache module in the Apache HTTP Server before 2.4.11 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty HTTP Content-Type header.
CVE-2014-3583	The handle_headers function in mod_proxy_fcgi.c in the mod_proxy_fcgi module in the Apache HTTP Server 2.4.10 allows remote FastCGI servers to cause a denial of service (buffer over-read and daemon crash) via long response headers.
CVE-2014-3587	Integer overflow in the cdf_read_property_info function in cdf.c in file through 5.19, as used in the Fileinfo component in PHP before 5.4.32 and 5.5.x before 5.5.16, allows remote attackers to cause a denial of service (application crash) via a crafted CDF file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-1571.

CVE-2014-3591	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-3596	The getCN function in Apache Axis 1.4 and earlier does not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via a certificate with a subject that specifies a common name in a field that is not the CN field. NOTE: this issue exists because of an incomplete fix for CVE-2012-5784.
CVE-2014-3609	HttpHdrRange.cc in Squid 3.x before 3.3.12 and 3.4.x before 3.4.6 allows remote attackers to cause a denial of service (crash) via a request with crafted "Range headers with unidentifiable byte-range values."
CVE-2014-3613	cURL and libcurl before 7.38.0 does not properly handle IP addresses in cookie domain names, which allows remote attackers to set cookies for or send arbitrary cookies to certain sites, as demonstrated by a site at 192.168.0.1 setting cookies for a site at 127.168.0.1.
CVE-2014-3616	nginx 0.5.6 through 1.7.4, when using the same shared ssl_session_cache or ssl_session_ticket_key for multiple servers, can reuse a cached SSL session for an unrelated context, which allows remote attackers with certain privileges to conduct "virtual host confusion" attacks.
CVE-2014-3618	Heap-based buffer overflow in formisc.c in formail in procmail 3.22 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted email header, related to "unbalanced quotes."
CVE-2014-3620	cURL and libcurl before 7.38.0 allow remote attackers to bypass the Same Origin Policy and set cookies for arbitrary sites by setting a cookie for a top-level domain.
CVE-2014-3634	rsyslog before 7.6.6 and 8.x before 8.4.1 and sysklogd 1.5 and earlier allows remote attackers to cause a denial of service (crash), possibly execute arbitrary code, or have other unspecified impact via a crafted priority (PRI) value that triggers an out-of-bounds array access.
CVE-2014-3660	parser.c in libxml2 before 2.9.2 does not properly prevent entity expansion even when entity substitution has been disabled, which allows context-dependent attackers to cause a denial of service (CPU consumption) via a crafted XML document containing

	a large number of nested entity references, a variant of the "billion laughs" attack.
CVE-2014-3668	Buffer overflow in the date_from_ISO8601 function in the mkgmtime implementation in libxmlrpc/xmlrpc.c in the XMLRPC extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) via (1) a crafted first argument to the xmlrpc_set_type function or (2) a crafted argument to the xmlrpc_decode function, related to an out-of-bounds read operation.
CVE-2014-3669	Integer overflow in the object_custom function in ext/standard/var_unserializer.c in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an argument to the unserialize function that triggers calculation of a large length value.
CVE-2014-3670	The exif_ifd_make_value function in exif.c in the EXIF extension in PHP before 5.4.34, 5.5.x before 5.5.18, and 5.6.x before 5.6.2 operates on floating-point arrays incorrectly, which allows remote attackers to cause a denial of service (heap memory corruption and application crash) or possibly execute arbitrary code via a crafted JPEG image with TIFF thumbnail data that is improperly handled by the exif_thumbnail function.
CVE-2014-3707	The curl_easy_duphandle function in libcurl 7.17.1 through 7.38.0, when running with the CURLOPT_COPYPOSTFIELDS option, does not properly copy HTTP POST data for an easy handle, which triggers an out-of-bounds read that allows remote web servers to read sensitive memory information.
CVE-2014-3710	The donote function in readelf.c in file through 5.20, as used in the Fileinfo component in PHP 5.4.34, does not ensure that sufficient note headers are present, which allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted ELF file.
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-2014-3981	acinclude.m4, as used in the configure script in PHP 5.5.13 and earlier, allows local users to overwrite arbitrary files via a symlink attack on the /tmp/phpglibccheck file.
CVE-2014-4000	** RESERVED **

	This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-4002	Multiple cross-site scripting (XSS) vulnerabilities in Cacti 0.8.8b allow remote attackers to inject arbitrary web script or HTML via the (1) drp_action parameter to cdef.php, (2) data_input.php, (3) data_queries.php, (4) data_sources.php, (5) data_templates.php, (6) graph_templates.php, (7) graphs.php, (8) host.php, or (9) host_templates.php or the (10) graph_template_input_id or (11) graph_template_id parameter to graph_templates_inputs.php.
CVE-2014-4014	The capabilities implementation in the Linux kernel before 3.14.8 does not properly consider that namespaces are inapplicable to inodes, which allows local users to bypass intended chmod restrictions by first creating a user namespace, as demonstrated by setting the setgid bit on a file with group ownership of root.
CVE-2014-4049	Heap-based buffer overflow in the php_parserr function in ext/standard/dns.c in PHP 5.6.0beta4 and earlier allows remote servers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted DNS TXT record, related to the dns_get_record function.
CVE-2014-4209	Unspecified vulnerability in Oracle Java SE 5.0u65, 6u75, 7u60, and 8u5 allows remote attackers to affect confidentiality and integrity via vectors related to JMX.
CVE-2014-4216	Unspecified vulnerability in Oracle Java SE 5.0u65, 6u75, 7u60, and 8u5 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot.
CVE-2014-4218	Unspecified vulnerability in Oracle Java SE 5.0u65, 6u75, 7u60, and 8u5 allows remote attackers to affect integrity via unknown vectors related to Libraries.
CVE-2014-4219	Unspecified vulnerability in Oracle Java SE 6u75, 7u60, and 8u5 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot.
CVE-2014-4221	Unspecified vulnerability in Oracle Java SE 7u60 and 8u5 allows remote attackers to affect confidentiality via unknown vectors related to Libraries.
CVE-2014-4223	Unspecified vulnerability in Oracle Java SE 7u60 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2014-2483.

CVE-2014-4244	Unspecified vulnerability in Oracle Java SE 5.0u65, 6u75, 7u60, and 8u5, and JRockit R27.8.2 and JRockit R28.3.2, allows remote attackers to affect confidentiality and integrity via unknown vectors related to Security.
CVE-2014-4252	Unspecified vulnerability in Oracle Java SE 5.0u65, 6u75, 7u60, and 8u5 allows remote attackers to affect confidentiality via unknown vectors related to Security.
CVE-2014-4262	Unspecified vulnerability in Oracle Java SE 5.0u65, 6u75, 7u60, and 8u5 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.
CVE-2014-4263	Unspecified vulnerability in Oracle Java SE 5.0u65, 6u75, 7u60, and 8u5, and JRockit R27.8.2 and R28.3.2, allows remote attackers to affect confidentiality and integrity via unknown vectors related to "Diffie-Hellman key agreement."
CVE-2014-4266	Unspecified vulnerability in Oracle Java SE 7u60 and 8u5 allows remote attackers to affect integrity via unknown vectors related to Serviceability.
CVE-2014-4341	MIT Kerberos 5 (aka krb5) before 1.12.2 allows remote attackers to cause a denial of service (buffer over-read and application crash) by injecting invalid tokens into a GSSAPI application session.
CVE-2014-4342	MIT Kerberos 5 (aka krb5) 1.7.x through 1.12.x before 1.12.2 allows remote attackers to cause a denial of service (buffer over-read or NULL pointer dereference, and application crash) by injecting invalid tokens into a GSSAPI application session.
CVE-2014-4343	Double free vulnerability in the init_ctx_reselect function in the SPNEGO initiator in lib/gssapi/spnego/spnego_mech.c in MIT Kerberos 5 (aka krb5) 1.10.x through 1.12.x before 1.12.2 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via network traffic that appears to come from an intended acceptor, but specifies a security mechanism different from the one proposed by the initiator.
CVE-2014-4344	The acc_ctx_cont function in the SPNEGO acceptor in lib/gssapi/spnego/spnego_mech.c in MIT Kerberos 5 (aka krb5) 1.5.x through 1.12.x before 1.12.2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an empty continuation token at a certain point during a SPNEGO negotiation.
CVE-2014-4345	Off-by-one error in the krb5_encode_krbsecretkey function in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in the LDAP KDB module in kadmind in MIT Kerberos 5 (aka krb5) 1.6.x through 1.11.x before 1.11.6 and 1.12.x before 1.12.2 allows remote authenticated users to cause a denial of service (buffer

	overflow) or possibly execute arbitrary code via a series of "cpw -keepold" commands.
CVE-2014-4508	arch/x86/kernel/entry_32.S in the Linux kernel through 3.15.1 on 32-bit x86 platforms, when syscall auditing is enabled and the sep CPU feature flag is set, allows local users to cause a denial of service (OOPS and system crash) via an invalid syscall number, as demonstrated by number 1000.
CVE-2014-4607	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-4608	** DISPUTED ** Multiple integer overflows in the lzo1x_decompress_safe function in lib/lzo/lzo1x_decompress_safe.c in the LZO decompressor in the Linux kernel before 3.15.2 allow context-dependent attackers to cause a denial of service (memory corruption) via a crafted Literal Run. NOTE: the author of the LZO algorithms says "the Linux kernel is *not* affected; media hype."
CVE-2014-4616	Array index error in the scanstring function in the _json module in Python 2.7 through 3.5 and simplejson before 2.6.1 allows context-dependent attackers to read arbitrary process memory via a negative index value in the idx argument to the raw_decode function.
CVE-2014-4617	The do_uncompress function in g10/compress.c in GnuPG 1.x before 1.4.17 and 2.x before 2.0.24 allows context-dependent attackers to cause a denial of service (infinite loop) via malformed compressed packets, as demonstrated by an a3 01 5b ff byte sequence.
CVE-2014-4650	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
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-2014-4877	Absolute path traversal vulnerability in GNU Wget before 1.16, when recursion is enabled, allows remote FTP servers to write to arbitrary files, and consequently execute arbitrary code, via a LIST response that references the same filename within two entries, one of which indicates that the filename is for a symlink.
CVE-2014-4909	Integer overflow in the tr_bitfieldEnsureNthBitAlloced function in bitfield.c in Transmission before 2.84 allows remote attackers to cause a denial of service and possibly execute arbitrary code via a crafted peer message, which triggers an out-of-bounds write.
CVE-2014-4914	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-5008	Snoopy allows remote attackers to execute arbitrary commands.
CVE-2014-5009	Snoopy allows remote attackers to execute arbitrary commands. NOTE: this vulnerability exists due to an incomplete fix for CVE-2014-5008.
CVE-2014-5025	Cross-site scripting (XSS) vulnerability in data_sources.php in Cacti 0.8.8b allows remote authenticated users with console access to inject arbitrary web script or HTML via the name_cache parameter in a ds_edit action.
CVE-2014-5026	Multiple cross-site scripting (XSS) vulnerabilities in Cacti 0.8.8b allow remote authenticated users with console access to inject arbitrary web script or HTML via a (1) Graph Tree Title in a delete or (2) edit action; (3) CDEF Name, (4) Data Input Method Name, or (5) Host Templates Name in a delete action; (6) Data Source Title; (7) Graph Title; or (8) Graph Template Name in a delete or (9) duplicate action.
CVE-2014-5029	The web interface in CUPS 1.7.4 allows local users in the lp group to read arbitrary files via a symlink attack on a file in /var/cache/cups/rss/ and language[0] set to null. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-3537.
CVE-2014-5030	CUPS before 2.0 allows local users to read arbitrary files via a symlink attack on (1) index.html, (2) index.class, (3) index.pl, (4) index.php, (5) index.pyc, or (6) index.py.
CVE-2014-5031	The web interface in CUPS before 2.0 does not check that files have world-readable permissions, which allows remote attackers to obtains sensitive information via unspecified vectors.

CVE-2014-5119	Off-by-one error in the __gconv_translit_find function in gconv_trans.c in GNU C Library (aka glibc) allows context-dependent attackers to cause a denial of service (crash) or execute arbitrary code via vectors related to the CHARSET environment variable and gconv transliteration modules.
CVE-2014-5120	gd_ctx.c in the GD component in PHP 5.4.x before 5.4.32 and 5.5.x before 5.5.16 does not ensure that pathnames lack %00 sequences, which might allow remote attackers to overwrite arbitrary files via crafted input to an application that calls the (1) imagegd, (2) imagegd2, (3) imagegif, (4) imagejpeg, (5) imagepng, (6) imagewbmp, or (7) imagewebp function.
CVE-2014-5139	The ssl_set_client_disabled function in t1_lib.c in OpenSSL 1.0.1 before 1.0.1i allows remote SSL servers to cause a denial of service (NULL pointer dereference and client application crash) via a ServerHello message that includes an SRP ciphersuite without the required negotiation of that ciphersuite with the client.
CVE-2014-5206	The do_remount function in fs/namespace.c in the Linux kernel through 3.16.1 does not maintain the MNT_LOCK_READONLY bit across a remount of a bind mount, which allows local users to bypass an intended read-only restriction and defeat certain sandbox protection mechanisms via a "mount -o remount" command within a user namespace.
CVE-2014-5207	fs/namespace.c in the Linux kernel through 3.16.1 does not properly restrict clearing MNT_NODEV, MNT_NOSUID, and MNT_NOEXEC and changing MNT_ATIME_MASK during a remount of a bind mount, which allows local users to gain privileges, interfere with backups and auditing on systems that had atime enabled, or cause a denial of service (excessive filesystem updating) on systems that had atime disabled via a "mount -o remount" command within a user namespace.
CVE-2014-5270	Libgcrypt before 1.5.4, as used in GnuPG and other products, does not properly perform ciphertext normalization and ciphertext randomization, which makes it easier for physically proximate attackers to conduct key-extraction attacks by leveraging the ability to collect voltage data from exposed metal, a different vector than CVE-2013-4576.
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-2014-5352	The krb5_gss_process_context_token function in lib/gssapi/krb5/process_context_token.c in the libgssapi_krb5 library in MIT Kerberos 5 (aka krb5) through 1.11.5, 1.12.x through 1.12.2, and 1.13.x before 1.13.1 does not properly maintain security-context handles, which allows remote authenticated users to cause a denial of service (use-after-free and double free, and daemon crash) or possibly execute arbitrary code via crafted GSSAPI traffic, as demonstrated by traffic to kadmind.
CVE-2014-5353	The krb5_ldap_get_password_policy_from_dn function in plugins/kdb/ldap/libkdb_ldap/ldap_pwd_policy.c in MIT Kerberos 5 (aka krb5) before 1.13.1, when the KDC uses LDAP, allows remote authenticated users to cause a denial of service (daemon crash) via a successful LDAP query with no results, as demonstrated by using an incorrect object type for a password policy.
CVE-2014-5355	MIT Kerberos 5 (aka krb5) through 1.13.1 incorrectly expects that a krb5_read_message data field is represented as a string ending with a '\0' character, which allows remote attackers to (1) cause a denial of service (NULL pointer dereference) via a zero-byte version string or (2) cause a denial of service (out-of-bounds read) by omitting the '\0' character, related to appl/user_user/server.c and lib/krb5/krb/recvauth.c.
CVE-2014-5461	Buffer overflow in the vararg functions in ldo.c in Lua 5.1 through 5.2.x before 5.2.3 allows context-dependent attackers to cause a denial of service (crash) via a small number of arguments to a function with a large number of fixed arguments.
CVE-2014-6040	GNU C Library (aka glibc) before 2.20 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via a multibyte character value of "0xffff" to the iconv function when converting (1) IBM933, (2) IBM935, (3) IBM937, (4) IBM939, or (5) IBM1364 encoded data to UTF-8.
CVE-2014-6271	GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid

	modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.
CVE-2014-6407	Docker before 1.3.2 allows remote attackers to write to arbitrary files and execute arbitrary code via a (1) symlink or (2) hard link attack in an image archive in a (a) pull or (b) load operation.
CVE-2014-6408	Docker 1.3.0 through 1.3.1 allows remote attackers to modify the default run profile of image containers and possibly bypass the container by applying unspecified security options to an image.
CVE-2014-6421	Use-after-free vulnerability in the SDP dissector in Wireshark 1.10.x before 1.10.10 allows remote attackers to cause a denial of service (application crash) via a crafted packet that leverages split memory ownership between the SDP and RTP dissectors.
CVE-2014-6422	The SDP dissector in Wireshark 1.10.x before 1.10.10 creates duplicate hashtables for a media channel, which allows remote attackers to cause a denial of service (application crash) via a crafted packet to the RTP dissector.
CVE-2014-6423	The tvb_raw_text_add function in epan/dissectors/packet-megaco.c in the MEGACO dissector in Wireshark 1.10.x before 1.10.10 and 1.12.x before 1.12.1 allows remote attackers to cause a denial of service (infinite loop) via an empty line.
CVE-2014-6424	The dissect_v9_v10_pdu_data function in epan/dissectors/packet-netflow.c in the Netflow dissector in Wireshark 1.10.x before 1.10.10 and 1.12.x before 1.12.1 refers to incorrect offset and start variables, which allows remote attackers to cause a denial of service (uninitialized memory read and application crash) via a crafted packet.
CVE-2014-6425	The (1) get_quoted_string and (2) get_unquoted_string functions in epan/dissectors/packet-cups.c in the CUPS dissector in Wireshark 1.12.x before 1.12.1 allow remote attackers to cause a denial of service (buffer over-read and application crash) via a CUPS packet that lacks a trailing '\0' character.
CVE-2014-6426	The dissect_hip_tlv function in epan/dissectors/packet-hip.c in the HIP dissector in Wireshark 1.12.x before 1.12.1 does not properly handle a NULL tree, which allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.
CVE-2014-6427	Off-by-one error in the is_rtsp_request_or_reply function in epan/dissectors/packet-rtsp.c in the RTSP

	dissector in Wireshark 1.10.x before 1.10.10 and 1.12.x before 1.12.1 allows remote attackers to cause a denial of service (application crash) via a crafted packet that triggers parsing of a token located one position beyond the current position.
CVE-2014-6428	The dissect_spdu function in epan/dissectors/packet-ses.c in the SES dissector in Wireshark 1.10.x before 1.10.10 and 1.12.x before 1.12.1 does not initialize a certain ID value, which allows remote attackers to cause a denial of service (application crash) via a crafted packet.
CVE-2014-6429	The SnifferDecompress function in wiretap/ngsniffer.c in the DOS Sniffer file parser in Wireshark 1.10.x before 1.10.10 and 1.12.x before 1.12.1 does not properly handle empty input data, which allows remote attackers to cause a denial of service (application crash) via a crafted file.
CVE-2014-6430	The SnifferDecompress function in wiretap/ngsniffer.c in the DOS Sniffer file parser in Wireshark 1.10.x before 1.10.10 and 1.12.x before 1.12.1 does not validate bitmask data, which allows remote attackers to cause a denial of service (application crash) via a crafted file.
CVE-2014-6431	Buffer overflow in the SnifferDecompress function in wiretap/ngsniffer.c in the DOS Sniffer file parser in Wireshark 1.10.x before 1.10.10 and 1.12.x before 1.12.1 allows remote attackers to cause a denial of service (application crash) via a crafted file that triggers writes of uncompressed bytes beyond the end of the output buffer.
CVE-2014-6432	The SnifferDecompress function in wiretap/ngsniffer.c in the DOS Sniffer file parser in Wireshark 1.10.x before 1.10.10 and 1.12.x before 1.12.1 does not prevent data overwrites during copy operations, which allows remote attackers to cause a denial of service (application crash) via a crafted file.
CVE-2014-6457	Unspecified vulnerability in Oracle Java SE 5.0u71, 6u81, 7u67, and 8u20; Java SE Embedded 7u60; and JRockit R27.8.3, and R28.3.3 allows remote attackers to affect confidentiality and integrity via vectors related to JSSE.
CVE-2014-6468	Unspecified vulnerability in Oracle Java SE 8u20 allows local users to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot.
CVE-2014-6491	Unspecified vulnerability in Oracle MySQL Server 5.5.39 and earlier and 5.6.20 and earlier allows remote attackers to affect confidentiality, integrity, and availability via vectors related to SERVER:SSL:yaSSL, a different vulnerability than CVE-2014-6500.
CVE-2014-6494	Unspecified vulnerability in Oracle MySQL Server 5.5.39 and earlier, and 5.6.20 and earlier, allows remote

	attackers to affect availability via vectors related to CLIENT:SSL:yaSSL, a different vulnerability than CVE-2014-6496.
CVE-2014-6500	Unspecified vulnerability in Oracle MySQL Server 5.5.39 and earlier, and 5.6.20 and earlier, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to SERVER:SSL:yaSSL, a different vulnerability than CVE-2014-6491.
CVE-2014-6502	Unspecified vulnerability in Oracle Java SE 5.0u71, 6u81, 7u67, and 8u20, and Java SE Embedded 7u60, allows remote attackers to affect integrity via unknown vectors related to Libraries.
CVE-2014-6504	Unspecified vulnerability in Oracle Java SE 5.0u71, 6u81, and 7u67, and Java SE Embedded 7u60, allows remote attackers to affect confidentiality via unknown vectors related to Hotspot.
CVE-2014-6506	Unspecified vulnerability in Oracle Java SE 5.0u71, 6u81, 7u67, and 8u20, and Java SE Embedded 7u60, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.
CVE-2014-6511	Unspecified vulnerability in Oracle Java SE 5.0u71, 6u81, 7u67, and 8u20 allows remote attackers to affect confidentiality via unknown vectors related to 2D.
CVE-2014-6512	Unspecified vulnerability in Oracle Java SE 5.0u71, 6u81, 7u67, and 8u20; Java SE Embedded 7u60; and JRockit R27.8.3 and R28.3.3 allows remote attackers to affect integrity via unknown vectors related to Libraries.
CVE-2014-6517	Unspecified vulnerability in Oracle Java SE 6u81, 7u67, and 8u20; Java SE Embedded 7u60; and Jrockit R27.8.3 and R28.3.3 allows remote attackers to affect confidentiality via vectors related to JAXP.
CVE-2014-6519	Unspecified vulnerability in Oracle Java SE 7u67 and 8u20, and Java SE Embedded 7u60, allows remote attackers to affect integrity via unknown vectors related to Hotspot.
CVE-2014-6531	Unspecified vulnerability in Oracle Java SE 5.0u71, 6u81, 7u67, and 8u20, and Java SE Embedded 7u60, allows remote attackers to affect confidentiality via unknown vectors related to Libraries.
CVE-2014-6549	Unspecified vulnerability in Oracle Java SE 8u25 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.
CVE-2014-6558	Unspecified vulnerability in Oracle Java SE 5.0u71, 6u81, 7u67, and 8u20; Java SE Embedded 7u60; and JRockit R27.8.3 and JRockit R28.3.3 allows remote attackers to affect integrity via unknown vectors related to Security.

CVE-2014-6559	Unspecified vulnerability in Oracle MySQL Server 5.5.39 and earlier, and 5.6.20 and earlier, allows remote attackers to affect confidentiality via vectors related to C API SSL CERTIFICATE HANDLING.
CVE-2014-6562	Unspecified vulnerability in Oracle Java SE 8u20 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.
CVE-2014-6585	Unspecified vulnerability in Oracle Java SE 5.0u75, 6u85, 7u72, and 8u25 allows remote attackers to affect confidentiality via unknown vectors related to 2D, a different vulnerability than CVE-2014-6591.
CVE-2014-6587	Unspecified vulnerability in Oracle Java SE 6u85, 7u72, and 8u25 allows local users to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.
CVE-2014-6591	Unspecified vulnerability in the Java SE component in Oracle Java SE 5.0u75, 6u85, 7u72, and 8u25 allows remote attackers to affect confidentiality via unknown vectors related to 2D, a different vulnerability than CVE-2014-6585.
CVE-2014-6593	Unspecified vulnerability in Oracle Java SE 5.0u75, 6u85, 7u72, and 8u25; Java SE Embedded 7u71 and 8u6; and JRockit 27.8.4 and 28.3.4 allows remote attackers to affect confidentiality and integrity via vectors related to JSSE.
CVE-2014-6601	Unspecified vulnerability in Oracle Java SE 6u85, 7u72, and 8u25 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot.
CVE-2014-7169	GNU Bash through 4.3 bash43-025 processes trailing strings after certain malformed function definitions in the values of environment variables, which allows remote attackers to write to files or possibly have unknown other impact via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-6271.
CVE-2014-7185	Integer overflow in bufferobject.c in Python before 2.7.8 allows context-dependent attackers to obtain sensitive information from process memory via a large size and offset in a "buffer" function.
CVE-2014-7186	The redirection implementation in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified

	other impact via crafted use of here documents, aka the "redir_stack" issue.
CVE-2014-7187	Off-by-one error in the read_token_word function in parse.y in GNU Bash through 4.3 bash43-026 allows remote attackers to cause a denial of service (out-of-bounds array access and application crash) or possibly have unspecified other impact via deeply nested for loops, aka the "word_lineno" issue.
CVE-2014-7189	crpyto/tls in Go 1.1 before 1.3.2, when SessionTicketsDisabled is enabled, allows man-in-the-middle attackers to spoof clients via unspecified vectors.
CVE-2014-7810	The Expression Language (EL) implementation in Apache Tomcat 6.x before 6.0.44, 7.x before 7.0.58, and 8.x before 8.0.16 does not properly consider the possibility of an accessible interface implemented by an inaccessible class, which allows attackers to bypass a SecurityManager protection mechanism via a web application that leverages use of incorrect privileges during EL evaluation.
CVE-2014-7817	The wordexp function in GNU C Library (aka glibc) 2.21 does not enforce the WRDE_NOCMD flag, which allows context-dependent attackers to execute arbitrary commands, as demonstrated by input containing "$((`...`))".
CVE-2014-7822	The implementation of certain splice_write file operations in the Linux kernel before 3.16 does not enforce a restriction on the maximum size of a single file, which allows local users to cause a denial of service (system crash) or possibly have unspecified other impact via a crafted splice system call, as demonstrated by use of a file descriptor associated with an ext4 filesystem.
CVE-2014-7841	The sctp_process_param function in net/sctp/sm_make_chunk.c in the SCTP implementation in the Linux kernel before 3.17.4, when ASCONF is used, allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) via a malformed INIT chunk.
CVE-2014-7844	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
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-2014-7970	The pivot_root implementation in fs/namespace.c in the Linux kernel through 3.17 does not properly interact with certain locations of a chroot directory, which allows local users to cause a denial of service (mount-tree loop) via . (dot) values in both arguments to the pivot_root system call.
CVE-2014-8080	The REXML parser in Ruby 1.9.x before 1.9.3-p550, 2.0.x before 2.0.0-p594, and 2.1.x before 2.1.4 allows remote attackers to cause a denial of service (memory consumption) via a crafted XML document, aka an XML Entity Expansion (XEE) attack.
CVE-2014-8088	The (1) Zend_Ldap class in Zend before 1.12.9 and (2) Zend\Ldap component in Zend 2.x before 2.2.8 and 2.3.x before 2.3.3 allows remote attackers to bypass authentication via a password starting with a null byte, which triggers an unauthenticated bind.
CVE-2014-8089	Zend Framework ZF2014-05 and ZF2014-06
CVE-2014-8090	The REXML parser in Ruby 1.9.x before 1.9.3 patchlevel 551, 2.0.x before 2.0.0 patchlevel 598, and 2.1.x before 2.1.5 allows remote attackers to cause a denial of service (CPU and memory consumption) a crafted XML document containing an empty string in an entity that is used in a large number of nested entity references, aka an XML Entity Expansion (XEE) attack. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-1821 and CVE-2014-8080.
CVE-2014-8091	X.Org X Window System (aka X11 and X) X11R5 and X.Org Server (aka xserver and xorg-server) before 1.16.3, when using SUN-DES-1 (Secure RPC)

	authentication credentials, does not check the return value of a malloc call, which allows remote attackers to cause a denial of service (NULL pointer dereference and server crash) via a crafted connection request.
CVE-2014-8092	Multiple integer overflows in X.Org X Window System (aka X11 or X) X11R1 and X.Org Server (aka xserver and xorg-server) before 1.16.3 allow remote authenticated users to cause a denial of service (crash) or possibly execute arbitrary code via a crafted request to the (1) ProcPutImage, (2) GetHosts, (3) RegionSizeof, or (4) REQUEST_FIXED_SIZE function, which triggers an out-of-bounds read or write.
CVE-2014-8093	Multiple integer overflows in the GLX extension in XFree86 4.0, X.Org X Window System (aka X11 or X) X11R6.7, and X.Org Server (aka xserver and xorg-server) before 1.16.3 allow remote authenticated users to cause a denial of service (crash) or possibly execute arbitrary code via a crafted request to the (1) __glXDisp_ReadPixels, (2) __glXDispSwap_ReadPixels, (3) __glXDisp_GetTexImage, (4) __glXDispSwap_GetTexImage, (5) GetSeparableFilter, (6) GetConvolutionFilter, (7) GetHistogram, (8) GetMinmax, (9) GetColorTable, (10) __glXGetAnswerBuffer, (11) __GLX_GET_ANSWER_BUFFER, (12) __glXMap1dReqSize, (13) __glXMap1fReqSize, (14) Map2Size, (15) __glXMap2dReqSize, (16) __glXMap2fReqSize, (17) __glXImageSize, or (18) __glXSeparableFilter2DReqSize function, which triggers an out-of-bounds read or write.
CVE-2014-8094	Integer overflow in the ProcDRI2GetBuffers function in the DRI2 extension in X.Org Server (aka xserver and xorg-server) 1.7.0 through 1.16.x before 1.16.3 allows remote authenticated users to cause a denial of service (crash) or possibly execute arbitrary code via a crafted request, which triggers an out-of-bounds read or write.
CVE-2014-8095	The XInput extension in X.Org X Window System (aka X11 or X) X11R4 and X.Org Server (aka xserver and xorg-server) before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value to the (1) SProcXChangeDeviceControl, (2) ProcXChangeDeviceControl, (3) ProcXChangeFeedbackControl, (4) ProcXSendExtensionEvent, (5) SProcXIAllowEvents, (6) SProcXIChangeCursor, (7) ProcXIChangeHierarchy, (8) SProcXIGetClientPointer, (9) SProcXIGrabDevice, (10) SProcXIUngrabDevice, (11) ProcXIUngrabDevice, (12) SProcXIPassiveGrabDevice, (13) ProcXIPassiveGrabDevice, (14)

	SProcXIPassiveUngrabDevice, (15) ProcXIPassiveUngrabDevice, (16) SProcXListDeviceProperties, (17) SProcXDeleteDeviceProperty, (18) SProcXIListProperties, (19) SProcXIDeleteProperty, (20) SProcXIGetProperty, (21) SProcXIQueryDevice, (22) SProcXIQueryPointer, (23) SProcXISelectEvents, (24) SProcXISetClientPointer, (25) SProcXISetFocus, (26) SProcXIGetFocus, or (27) SProcXIWarpPointer function.
CVE-2014-8096	The SProcXCMiscGetXIDList function in the XC-MISC extension in X.Org X Window System (aka X11 or X) X11R6.0 and X.Org Server (aka xserver and xorg-server) before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value.
CVE-2014-8097	The DBE extension in X.Org X Window System (aka X11 or X) X11R6.1 and X.Org Server (aka xserver and xorg-server) before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value to the (1) ProcDbeSwapBuffers or (2) SProcDbeSwapBuffers function.
CVE-2014-8098	The GLX extension in XFree86 4.0, X.Org X Window System (aka X11 or X) X11R6.7, and X.Org Server (aka xserver and xorg-server) before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value to the (1) __glXDisp_Render, (2) __glXDisp_RenderLarge, (3) __glXDispSwap_VendorPrivate, (4) __glXDispSwap_VendorPrivateWithReply, (5) set_client_info, (6) __glXDispSwap_SetClientInfoARB, (7) DoSwapInterval, (8) DoGetProgramString, (9) DoGetString, (10) __glXDispSwap_RenderMode, (11) __glXDisp_GetCompressedTexImage, (12) __glXDispSwap_GetCompressedTexImage, (13) __glXDisp_FeedbackBuffer, (14) __glXDispSwap_FeedbackBuffer, (15) __glXDisp_SelectBuffer, (16) __glXDispSwap_SelectBuffer, (17) __glXDisp_Flush, (18) __glXDispSwap_Flush, (19) __glXDisp_Finish, (20) __glXDispSwap_Finish, (21) __glXDisp_ReadPixels, (22) __glXDispSwap_ReadPixels, (23) __glXDisp_GetTexImage, (24) __glXDispSwap_GetTexImage, (25) __glXDisp_GetPolygonStipple, (26) __glXDispSwap_GetPolygonStipple, (27) __glXDisp_GetSeparableFilter, (28) __glXDisp_GetSeparableFilterEXT, (29)

	__glXDisp_GetConvolutionFilter, (30) __glXDisp_GetConvolutionFilterEXT, (31) __glXDisp_GetHistogram, (32) __glXDisp_GetHistogramEXT, (33) __glXDisp_GetMinmax, (34) __glXDisp_GetMinmaxEXT, (35) __glXDisp_GetColorTable, (36) __glXDisp_GetColorTableSGI, (37) GetSeparableFilter, (38) GetConvolutionFilter, (39) GetHistogram, (40) GetMinmax, or (41) GetColorTable function.
CVE-2014-8099	The XVideo extension in XFree86 4.0.0, X.Org X Window System (aka X11 or X) X11R6.7, and X.Org Server (aka xserver and xorg-server) before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value to the (1) SProcXvQueryExtension, (2) SProcXvQueryAdaptors, (3) SProcXvQueryEncodings, (4) SProcXvGrabPort, (5) SProcXvUngrabPort, (6) SProcXvPutVideo, (7) SProcXvPutStill, (8) SProcXvGetVideo, (9) SProcXvGetStill, (10) SProcXvPutImage, (11) SProcXvShmPutImage, (12) SProcXvSelectVideoNotify, (13) SProcXvSelectPortNotify, (14) SProcXvStopVideo, (15) SProcXvSetPortAttribute, (16) SProcXvGetPortAttribute, (17) SProcXvQueryBestSize, (18) SProcXvQueryPortAttributes, (19) SProcXvQueryImageAttributes, or (20) SProcXvListImageFormats function.
CVE-2014-8100	The Render extension in XFree86 4.0.1, X.Org X Window System (aka X11 or X) X11R6.7, and X.Org Server (aka xserver and xorg-server) before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value to the (1) ProcRenderQueryVersion, (2) SProcRenderQueryVersion, (3) SProcRenderQueryPictFormats, (4) SProcRenderQueryPictIndexValues, (5) SProcRenderCreatePicture, (6) SProcRenderChangePicture, (7) SProcRenderSetPictureClipRectangles, (8) SProcRenderFreePicture, (9) SProcRenderComposite, (10) SProcRenderScale, (11) SProcRenderCreateGlyphSet, (12) SProcRenderReferenceGlyphSet, (13) SProcRenderFreeGlyphSet, (14) SProcRenderFreeGlyphs, or (15) SProcRenderCompositeGlyphs function.
CVE-2014-8101	The RandR extension in XFree86 4.2.0, X.Org X Window System (aka X11 or X) X11R6.7, and X.Org Server (aka xserver and xorg-server) before

	1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value to the (1) SProcRRQueryVersion, (2) SProcRRGetScreenInfo, (3) SProcRRSelectInput, or (4) SProcRRConfigureOutputProperty function.
CVE-2014-8102	The SProcXFixesSelectSelectionInput function in the XFixes extension in X.Org X Window System (aka X11 or X) X11R6.8.0 and X.Org Server (aka xserver and xorg-server) before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length value.
CVE-2014-8103	X.Org Server (aka xserver and xorg-server) 1.15.0 through 1.16.x before 1.16.3 allows remote authenticated users to cause a denial of service (out-of-bounds read or write) or possibly execute arbitrary code via a crafted length or index value to the (1) sproc_dri3_query_version, (2) sproc_dri3_open, (3) sproc_dri3_pixmap_from_buffer, (4) sproc_dri3_buffer_from_pixmap, (5) sproc_dri3_fence_from_fd, (6) sproc_dri3_fd_from_fence, (7) proc_present_query_capabilities, (8) sproc_present_query_version, (9) sproc_present_pixmap, (10) sproc_present_notify_msc, (11) sproc_present_select_input, or (12) sproc_present_query_capabilities function in the (a) DRI3 or (b) Present extension.
CVE-2014-8104	OpenVPN 2.x before 2.0.11, 2.1.x, 2.2.x before 2.2.3, and 2.3.x before 2.3.6 allows remote authenticated users to cause a denial of service (server crash) via a small control channel packet.
CVE-2014-8105	389 Directory Server before 1.3.2.27 and 1.3.3.x before 1.3.3.9 does not properly restrict access to the "cn=changelog" LDAP sub-tree, which allows remote attackers to obtain sensitive information from the changelog via unspecified vectors.
CVE-2014-8108	The mod_dav_svn Apache HTTPD server module in Apache Subversion 1.7.x before 1.7.19 and 1.8.x before 1.8.11 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a request for a URI that triggers a lookup for a virtual transaction name that does not exist.
CVE-2014-8109	mod_lua.c in the mod_lua module in the Apache HTTP Server 2.3.x and 2.4.x through 2.4.10 does not support an httpd configuration in which the same Lua authorization provider is used with different arguments within different contexts, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging multiple

	Require directives, as demonstrated by a configuration that specifies authorization for one group to access a certain directory, and authorization for a second group to access a second directory.
CVE-2014-8112	389 Directory Server 1.3.1.x, 1.3.2.x before 1.3.2.27, and 1.3.3.x before 1.3.3.9 stores "unhashed" passwords even when the nsslapd-unhashed-pw-switch option is set to off, which allows remote authenticated users to obtain sensitive information by reading the Changelog.
CVE-2014-8116	The ELF parser (readelf.c) in file before 5.21 allows remote attackers to cause a denial of service (CPU consumption or crash) via a large number of (1) program or (2) section headers or (3) invalid capabilities.
CVE-2014-8117	softmagic.c in file before 5.21 does not properly limit recursion, which allows remote attackers to cause a denial of service (CPU consumption or crash) via unspecified vectors.
CVE-2014-8118	Integer overflow in RPM 4.12 and earlier allows remote attackers to execute arbitrary code via a crafted CPIO header in the payload section of an RPM file, which triggers a stack-based buffer overflow.
CVE-2014-8121	DB_LOOKUP in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6) 2.21 and earlier does not properly check if a file is open, which allows remote attackers to cause a denial of service (infinite loop) by performing a look-up on a database while iterating over it, which triggers the file pointer to be reset.
CVE-2014-8127	LibTIFF 4.0.3 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted TIFF image to the (1) checkInkNamesString function in tif_dir.c in the thumbnail tool, (2) compresscontig function in tiff2bw.c in the tiff2bw tool, (3) putcontig8bitCIELab function in tif_getimage.c in the tiff2rgba tool, LZWPreDecode function in tif_lzw.c in the (4) tiff2ps or (5) tiffdither tool, (6) NeXTDecode function in tif_next.c in the tiffmedian tool, or (7) TIFFWriteDirectoryTagLongLong8Array function in tif_dirwrite.c in the tiffset tool.
CVE-2014-8129	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-8130	** RESERVED **

	This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-8137	Double free vulnerability in the jas_iccattrval_destroy function in JasPer 1.900.1 and earlier allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted ICC color profile in a JPEG 2000 image file.
CVE-2014-8138	Heap-based buffer overflow in the jp2_decode function in JasPer 1.900.1 and earlier allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted JPEG 2000 file.
CVE-2014-8139	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-8140	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-8141	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-8142	Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.36, 5.5.x before 5.5.20, and 5.6.x before 5.6.4 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages improper handling of duplicate keys within the serialized properties of an object, a different vulnerability than CVE-2004-1019.
CVE-2014-8150	CRLF injection vulnerability in libcurl 6.0 through 7.x before 7.40.0, when using an HTTP proxy, allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via CRLF sequences in a URL.
CVE-2014-8155	GnuTLS before 2.9.10 does not verify the activation and expiration dates of CA certificates, which allows man-in-the-middle attackers to spoof servers via a certificate issued by a CA certificate that is (1) not yet valid or (2) no longer valid.

CVE-2014-8157	Off-by-one error in the jpc_dec_process_sot function in JasPer 1.900.1 and earlier allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted JPEG 2000 image, which triggers a heap-based buffer overflow.
CVE-2014-8158	Multiple stack-based buffer overflows in jpc_qmfb.c in JasPer 1.900.1 and earlier allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted JPEG 2000 image.
CVE-2014-8161	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-8169	automount 5.0.8, when a program map uses certain interpreted languages, uses the calling user's USER and HOME environment variable values instead of the values for the user used to run the mapped program, which allows local users to gain privileges via a Trojan horse program in the user home directory.
CVE-2014-8176	The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.
CVE-2014-8240	Integer overflow in TigerVNC allows remote VNC servers to cause a denial of service (crash) and possibly execute arbitrary code via vectors related to screen size handling, which triggers a heap-based buffer overflow, a similar issue to CVE-2014-6051.
CVE-2014-8241	XRegion in TigerVNC allows remote VNC servers to cause a denial of service (NULL pointer dereference) by leveraging failure to check a malloc return value, a similar issue to CVE-2014-6052.
CVE-2014-8275	OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k does not enforce certain constraints on certificate data, which allows remote attackers to defeat a fingerprint-based certificate-blacklist protection mechanism by including crafted data within a certificate's unsigned portion, related to crypto/asn1/a_verify.c, crypto/dsa/dsa_asn1.c, crypto/ecdsa/ecs_vrf.c, and crypto/x509/x_all.c.
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-2014-8484	The srec_scan function in bfd/srec.c in libdbfd in GNU binutils before 2.25 allows remote attackers to cause a denial of service (out-of-bounds read) via a small S-record.
CVE-2014-8485	The setup_group function in bfd/elf.c in libbfd in GNU binutils 2.24 and earlier allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via crafted section group headers in an ELF file.
CVE-2014-8500	ISC BIND 9.0.x through 9.8.x, 9.9.0 through 9.9.6, and 9.10.0 through 9.10.1 does not limit delegation chaining, which allows remote attackers to cause a denial of service (memory consumption and named crash) via a large or infinite number of referrals.
CVE-2014-8501	The _bfd_XXi_swap_aouthdr_in function in bfd/peXXigen.c in GNU binutils 2.24 and earlier allows remote attackers to cause a denial of service (out-of-bounds write) and possibly have other unspecified impact via a crafted NumberOfRvaAndSizes field in the AOUT header in a PE executable.
CVE-2014-8502	Heap-based buffer overflow in the pe_print_edata function in bfd/peXXigen.c in GNU binutils 2.24 and earlier allows remote attackers to cause a denial of service (crash) and possibly have other unspecified impact via a truncated export table in a PE file.
CVE-2014-8503	Stack-based buffer overflow in the ihex_scan function in bfd/ihex.c in GNU binutils 2.24 and earlier allows remote attackers to cause a denial of service (crash) and possibly have other unspecified impact via a crafted ihex file.
CVE-2014-8504	Stack-based buffer overflow in the srec_scan function in bfd/srec.c in GNU binutils 2.24 and earlier allows remote attackers to cause a denial of service (crash) and possibly have other unspecified impact via a crafted file.
CVE-2014-8710	The decompress_sigcomp_message function in epan/sigcomp-udvm.c in the SigComp UDVM dissector in Wireshark 1.10.x before 1.10.11 allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted packet.
CVE-2014-8711	Multiple integer overflows in epan/dissectors/packet-amqp.c in the AMQP dissector in Wireshark 1.10.x before 1.10.11 and 1.12.x before 1.12.2 allow remote attackers to cause a denial of service (application crash) via a crafted amqp_0_10 PDU in a packet.
CVE-2014-8712	The build_expert_data function in epan/dissectors/packet-ncp2222.inc in the NCP dissector in Wireshark 1.10.x before 1.10.11 and 1.12.x before 1.12.2 does not properly initialize a data structure, which allows remote

	attackers to cause a denial of service (application crash) via a crafted packet.
CVE-2014-8713	Stack-based buffer overflow in the build_expert_data function in epan/dissectors/packet-ncp2222.inc in the NCP dissector in Wireshark 1.10.x before 1.10.11 and 1.12.x before 1.12.2 allows remote attackers to cause a denial of service (application crash) via a crafted packet.
CVE-2014-8714	The dissect_write_structured_field function in epan/dissectors/packet-tn5250.c in the TN5250 dissector in Wireshark 1.10.x before 1.10.11 and 1.12.x before 1.12.2 allows remote attackers to cause a denial of service (infinite loop) via a crafted packet.
CVE-2014-8737	Multiple directory traversal vulnerabilities in GNU binutils 2.24 and earlier allow local users to delete arbitrary files via a .. (dot dot) or full path name in an archive to (1) strip or (2) objcopy or create arbitrary files via (3) a .. (dot dot) or full path name in an archive to ar.
CVE-2014-8738	The _bfd_slurp_extended_name_table function in bfd/archive.c in GNU binutils 2.24 and earlier allows remote attackers to cause a denial of service (invalid write, segmentation fault, and crash) via a crafted extended name table in an archive.
CVE-2014-8962	Stack-based buffer overflow in stream_decoder.c in libFLAC before 1.3.1 allows remote attackers to execute arbitrary code via a crafted .flac file.
CVE-2014-8964	Heap-based buffer overflow in PCRE 8.36 and earlier allows remote attackers to cause a denial of service (crash) or have other unspecified impact via a crafted regular expression, related to an assertion that allows zero repeats.
CVE-2014-8989	The Linux kernel through 3.17.4 does not properly restrict dropping of supplemental group memberships in certain namespace scenarios, which allows local users to bypass intended file permissions by leveraging a POSIX ACL containing an entry for the group category that is more restrictive than the entry for the other category, aka a "negative groups" issue, related to kernel/groups.c, kernel/uid16.c, and kernel/user_namespace.c.
CVE-2014-9028	Heap-based buffer overflow in stream_decoder.c in libFLAC before 1.3.1 allows remote attackers to execute arbitrary code via a crafted .flac file.
CVE-2014-9029	Multiple off-by-one errors in the (1) jpc_dec_cp_setfromcox and (2) jpc_dec_cp_setfromrgn functions in jpc/jpc_dec.c in JasPer 1.900.1 and earlier allow remote attackers to execute arbitrary code via a crafted jp2 file, which triggers a heap-based buffer overflow.

CVE-2014-9090	The do_double_fault function in arch/x86/kernel/traps.c in the Linux kernel through 3.17.4 does not properly handle faults associated with the Stack Segment (SS) segment register, which allows local users to cause a denial of service (panic) via a modify_ldt system call, as demonstrated by sigreturn_32 in the linux-clock-tests test suite.
CVE-2014-9092	libjpeg-turbo before 1.3.1 allows remote attackers to cause a denial of service (crash) via a crafted JPEG file, related to the Exif marker.
CVE-2014-9130	scanner.c in LibYAML 0.1.5 and 0.1.6, as used in the YAML-LibYAML (aka YAML-XS) module for Perl, allows context-dependent attackers to cause a denial of service (assertion failure and crash) via vectors involving line-wrapping.
CVE-2014-9157	Format string vulnerability in the yyerror function in lib/cgraph/scan.l in Graphviz allows remote attackers to have unspecified impact via format string specifiers in unknown vectors, which are not properly handled in an error string.
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-2014-9293	The config_auth function in ntpd in NTP before 4.2.7p11, when an auth key is not configured, improperly generates a key, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via a brute-force attack.
CVE-2014-9294	util/ntp-keygen.c in ntp-keygen in NTP before 4.2.7p230 uses a weak RNG seed, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via a brute-force attack.
CVE-2014-9295	Multiple stack-based buffer overflows in ntpd in NTP before 4.2.8 allow remote attackers to execute arbitrary code via a crafted packet, related to (1) the crypto_recv function when the Autokey Authentication feature is

	used, (2) the ctl_putdata function, and (3) the configure function.
CVE-2014-9296	The receive function in ntp_proto.c in ntpd in NTP before 4.2.8 continues to execute after detecting a certain authentication error, which might allow remote attackers to trigger an unintended association change via crafted packets.
CVE-2014-9322	arch/x86/kernel/entry_64.S in the Linux kernel before 3.17.5 does not properly handle faults associated with the Stack Segment (SS) segment register, which allows local users to gain privileges by triggering an IRET instruction that leads to access to a GS Base address from the wrong space.
CVE-2014-9328	ClamAV before 0.98.6 allows remote attackers to have unspecified impact via a crafted upack packer file, related to a "heap out of bounds condition."
CVE-2014-9330	Integer overflow in tif_packbits.c in bmp2tif in libtiff 4.0.3 allows remote attackers to cause a denial of service (crash) via crafted BMP image, related to dimensions, which triggers an out-of-bounds read.
CVE-2014-9356	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2014-9357	Docker 1.3.2 allows remote attackers to execute arbitrary code with root privileges via a crafted (1) image or (2) build in a Dockerfile in an LZMA (.xz) archive, related to the chroot for archive extraction.
CVE-2014-9358	Docker before 1.3.3 does not properly validate image IDs, which allows remote attackers to conduct path traversal attacks and spoof repositories via a crafted image in a (1) "docker load" operation or (2) "registry communications."
CVE-2014-9365	The HTTP clients in the (1) httplib, (2) urllib, (3) urllib2, and (4) xmlrpclib libraries in CPython (aka Python) 2.x before 2.7.9 and 3.x before 3.4.3, when accessing an HTTPS URL, do not (a) check the certificate against a trust store or verify that the server hostname matches a domain name in the subject's (b) Common Name or (c) subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.
CVE-2014-9421	The auth_gssapi_unwrap_data function in lib/rpc/auth_gssapi_misc.c in MIT Kerberos 5 (aka krb5) through 1.11.5, 1.12.x through 1.12.2, and 1.13.x before 1.13.1 does not properly handle partial XDR deserialization, which allows remote authenticated users to cause a denial of service (use-after-free

	and double free, and daemon crash) or possibly execute arbitrary code via malformed XDR data, as demonstrated by data sent to kadmind.
CVE-2014-9422	The check_rpcsec_auth function in kadmin/server/kadm_rpc_svc.c in kadmind in MIT Kerberos 5 (aka krb5) through 1.11.5, 1.12.x through 1.12.2, and 1.13.x before 1.13.1 allows remote authenticated users to bypass a kadmin/* authorization check and obtain administrative access by leveraging access to a two-component principal with an initial "kadmind" substring, as demonstrated by a "ka/x" principal.
CVE-2014-9427	sapi/cgi/cgi_main.c in the CGI component in PHP through 5.4.36, 5.5.x through 5.5.20, and 5.6.x through 5.6.4, when mmap is used to read a .php file, does not properly consider the mapping's length during processing of an invalid file that begins with a # character and lacks a newline character, which causes an out-of-bounds read and might (1) allow remote attackers to obtain sensitive information from php-cgi process memory by leveraging the ability to upload a .php file or (2) trigger unexpected code execution if a valid PHP script is present in memory locations adjacent to the mapping.
CVE-2014-9620	The ELF parser in file 5.08 through 5.21 allows remote attackers to cause a denial of service via a large number of notes.
CVE-2014-9621	The ELF parser in file 5.16 through 5.21 allows remote attackers to cause a denial of service via a long string.
CVE-2014-9636	unzip 6.0 allows remote attackers to cause a denial of service (out-of-bounds read or write and crash) via an extra field with an uncompressed size smaller than the compressed field size in a zip archive that advertises STORED method compression.
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-2014-9653	readelf.c in file before 5.22, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21,

	and 5.6.x before 5.6.5, does not consider that pread calls sometimes read only a subset of the available data, which allows remote attackers to cause a denial of service (uninitialized memory access) or possibly have unspecified other impact via a crafted ELF file.
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-2014-9655	The (1) putcontig8bitYCbCr21tile function in tif_getimage.c or (2) NeXTDecode function in tif_next.c in LibTIFF allows remote attackers to cause a denial of service (uninitialized memory access) via a crafted TIFF image, as demonstrated by libtiff-cvs-1.tif and libtiff-cvs-2.tif.
CVE-2014-9657	The tt_face_load_hdmx function in truetype/ttpload.c in FreeType before 2.5.4 does not establish a minimum record size, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted TrueType font.
CVE-2014-9658	The tt_face_load_kern function in sfnt/ttkern.c in FreeType before 2.5.4 enforces an incorrect minimum table length, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted TrueType font.
CVE-2014-9660	The _bdf_parse_glyphs function in bdf/bdflib.c in FreeType before 2.5.4 does not properly handle a missing ENDCHAR record, which allows remote attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via a crafted BDF font.
CVE-2014-9661	type42/t42parse.c in FreeType before 2.5.4 does not consider that scanning can be incomplete without triggering an error, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted Type42 font.
CVE-2014-9663	The tt_cmap4_validate function in sfnt/ttcmap.c in FreeType before 2.5.4 validates a certain length field before that field's value is completely calculated, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted cmap SFNT table.
CVE-2014-9664	FreeType before 2.5.4 does not check for the end of the data during certain parsing actions, which allows

	remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted Type42 font, related to type42/t42parse.c and type1/t1load.c.
CVE-2014-9667	sfnt/ttload.c in FreeType before 2.5.4 proceeds with offset+length calculations without restricting the values, which allows remote attackers to cause a denial of service (integer overflow and out-of-bounds read) or possibly have unspecified other impact via a crafted SFNT table.
CVE-2014-9669	Multiple integer overflows in sfnt/ttcmap.c in FreeType before 2.5.4 allow remote attackers to cause a denial of service (out-of-bounds read or memory corruption) or possibly have unspecified other impact via a crafted cmap SFNT table.
CVE-2014-9670	Multiple integer signedness errors in the pcf_get_encodings function in pcf/pcfread.c in FreeType before 2.5.4 allow remote attackers to cause a denial of service (integer overflow, NULL pointer dereference, and application crash) via a crafted PCF file that specifies negative values for the first column and first row.
CVE-2014-9671	Off-by-one error in the pcf_get_properties function in pcf/pcfread.c in FreeType before 2.5.4 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted PCF file with a 0xffffffff size value that is improperly incremented.
CVE-2014-9673	Integer signedness error in the Mac_Read_POST_Resource function in base/ftobjs.c in FreeType before 2.5.4 allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a crafted Mac font.
CVE-2014-9674	The Mac_Read_POST_Resource function in base/ftobjs.c in FreeType before 2.5.4 proceeds with adding to length values without validating the original values, which allows remote attackers to cause a denial of service (integer overflow and heap-based buffer overflow) or possibly have unspecified other impact via a crafted Mac font.
CVE-2014-9675	bdf/bdflib.c in FreeType before 2.5.4 identifies property names by only verifying that an initial substring is present, which allows remote attackers to discover heap pointer values and bypass the ASLR protection mechanism via a crafted BDF font.
CVE-2014-9679	Integer underflow in the cupsRasterReadPixels function in filter/raster.c in CUPS before 2.0.2 allows remote attackers to have unspecified impact via a malformed compressed raster file, which triggers a buffer overflow.

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-2014-9709	The GetCode_ function in gd_gif_in.c in GD 2.1.1 and earlier, as used in PHP before 5.5.21 and 5.6.x before 5.6.5, allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted GIF image that is improperly handled by the gdImageCreateFromGif function.
CVE-2014-9750	ntp_crypto.c in ntpd in NTP 4.x before 4.2.8p1, when Autokey Authentication is enabled, allows remote attackers to obtain sensitive information from process memory or cause a denial of service (daemon crash) via a packet containing an extension field with an invalid value for the length of its value field.
CVE-2014-9761	Multiple stack-based buffer overflows in the GNU C Library (aka glibc or libc6) before 2.23 allow context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long argument to the (1) nan, (2) nanf, or (3) nanl function.
CVE-2015-0202	The mod_dav_svn server in Subversion 1.8.0 through 1.8.11 allows remote attackers to cause a denial of service (memory consumption) via a large number of REPORT requests, which trigger the traversal of FSFS repository nodes.
CVE-2015-0204	The ssl3_get_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8zd, 1.0.0 before 1.0.0p, and 1.0.1 before 1.0.1k allows remote SSL servers to conduct RSA-to-EXPORT_RSA downgrade attacks and facilitate brute-force decryption by offering a weak ephemeral RSA key in a noncompliant role, related to the "FREAK" issue. NOTE: the scope of this CVE is only client code based on OpenSSL, not EXPORT_RSA issues associated with servers or other TLS implementations.
CVE-2015-0205	The ssl3_get_cert_verify function in s3_srvr.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k accepts client authentication with a Diffie-Hellman (DH) certificate without requiring a CertificateVerify message, which allows remote attackers to obtain access without knowledge of a private key via crafted TLS Handshake Protocol traffic to a server that recognizes a Certification Authority with DH support.

CVE-2015-0206	Memory leak in the dtls1_buffer_record function in d1_pkt.c in OpenSSL 1.0.0 before 1.0.0p and 1.0.1 before 1.0.1k allows remote attackers to cause a denial of service (memory consumption) by sending many duplicate records for the next epoch, leading to failure of replay detection.
CVE-2015-0209	Use-after-free vulnerability in the d2i_ECPrivateKey function in crypto/ec/ec_asn1.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a malformed Elliptic Curve (EC) private-key file that is improperly handled during import.
CVE-2015-0228	The lua_websocket_read function in lua_request.c in the mod_lua module in the Apache HTTP Server through 2.4.12 allows remote attackers to cause a denial of service (child-process crash) by sending a crafted WebSocket Ping frame after a Lua script has called the wsupgrade function.
CVE-2015-0231	Use-after-free vulnerability in the process_nested_data function in ext/standard/var_unserializer.re in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code via a crafted unserialize call that leverages improper handling of duplicate numerical keys within the serialized properties of an object. NOTE: this vulnerability exists because of an incomplete fix for CVE-2014-8142.
CVE-2015-0232	The exif_process_unicode function in ext/exif/exif.c in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5 allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized pointer free and application crash) via crafted EXIF data in a JPEG image.
CVE-2015-0235	Heap-based buffer overflow in the __nss_hostname_digits_dots function in glibc 2.2, and other 2.x versions before 2.18, allows context-dependent attackers to execute arbitrary code via vectors related to the (1) gethostbyname or (2) gethostbyname2 function, aka "GHOST."
CVE-2015-0241	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2015-0242	** RESERVED **

	This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2015-0243	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2015-0244	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2015-0247	Heap-based buffer overflow in openfs.c in the libext2fs library in e2fsprogs before 1.42.12 allows local users to execute arbitrary code via crafted block group descriptor data in a filesystem image.
CVE-2015-0248	The (1) mod_dav_svn and (2) svnserve servers in Subversion 1.6.0 through 1.7.19 and 1.8.0 through 1.8.11 allow remote attackers to cause a denial of service (assertion failure and abort) via crafted parameter combinations related to dynamically evaluated revision numbers.
CVE-2015-0251	The mod_dav_svn server in Subversion 1.5.0 through 1.7.19 and 1.8.0 through 1.8.11 allows remote authenticated users to spoof the svn:author property via a crafted v1 HTTP protocol request sequences.
CVE-2015-0253	The read_request_line function in server/protocol.c in the Apache HTTP Server 2.4.12 does not initialize the protocol structure member, which allows remote attackers to cause a denial of service (NULL pointer dereference and process crash) by sending a request that lacks a method to an installation that enables the INCLUDES filter and has an ErrorDocument 400 directive specifying a local URI.
CVE-2015-0254	Apache Standard Taglibs before 1.2.3 allows remote attackers to execute arbitrary code or conduct external XML entity (XXE) attacks via a crafted XSLT extension in a (1) <x:parse> or (2) <x:transform> JSTL XML tag.
CVE-2015-0255	X.Org Server (aka xserver and xorg-server) before 1.16.3 and 1.17.x before 1.17.1 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (crash) via a crafted string length value in a XkbSetGeometry request.
CVE-2015-0261	Integer signedness error in the mobility_opt_print function in the IPv6 mobility printer in tcpdump before

	4.7.2 allows remote attackers to cause a denial of service (out-of-bounds read and crash) or possibly execute arbitrary code via a negative length value.
CVE-2015-0273	Multiple use-after-free vulnerabilities in ext/date/php_date.c in PHP before 5.4.38, 5.5.x before 5.5.22, and 5.6.x before 5.6.6 allow remote attackers to execute arbitrary code via crafted serialized input containing a (1) R or (2) r type specifier in (a) DateTimeZone data handled by the php_date_timezone_initialize_from_hash function or (b) DateTime data handled by the php_date_initialize_from_hash function.
CVE-2015-0274	The XFS implementation in the Linux kernel before 3.15 improperly uses an old size value during remote attribute replacement, which allows local users to cause a denial of service (transaction overrun and data corruption) or possibly gain privileges by leveraging XFS filesystem access.
CVE-2015-0282	GnuTLS before 3.1.0 does not verify that the RSA PKCS #1 signature algorithm matches the signature algorithm in the certificate, which allows remote attackers to conduct downgrade attacks via unspecified vectors.
CVE-2015-0286	The ASN1_TYPE_cmp function in crypto/asn1/a_type.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly perform boolean-type comparisons, which allows remote attackers to cause a denial of service (invalid read operation and application crash) via a crafted X.509 certificate to an endpoint that uses the certificate-verification feature.
CVE-2015-0287	The ASN1_item_ex_d2i function in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not reinitialize CHOICE and ADB data structures, which might allow attackers to cause a denial of service (invalid write operation and memory corruption) by leveraging an application that relies on ASN.1 structure reuse.
CVE-2015-0288	The X509_to_X509_REQ function in crypto/x509/x509_req.c in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a might allow attackers to cause a denial of service (NULL pointer dereference and application crash) via an invalid certificate key.
CVE-2015-0289	The PKCS#7 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a does not properly handle a lack of outer ContentInfo, which allows attackers to cause a denial of service (NULL pointer dereference and application crash) by leveraging an application

	that processes arbitrary PKCS#7 data and providing malformed data with ASN.1 encoding, related to crypto/pkcs7/pk7_doit.c and crypto/pkcs7/pk7_lib.c.
CVE-2015-0292	Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.
CVE-2015-0293	The SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a allows remote attackers to cause a denial of service (s2_lib.c assertion failure and daemon exit) via a crafted CLIENT-MASTER-KEY message.
CVE-2015-0294	certificate algorithm consistency checking issue
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-2015-0383	Unspecified vulnerability in Oracle Java SE 5.0u75, 6u85, 7u72, and 8u25; Java SE Embedded 7u71 and 8u6; and JRockit R27.8.4 and R28.3.4 allows local users to affect integrity and availability via unknown vectors related to Hotspot.
CVE-2015-0395	Unspecified vulnerability in Oracle Java SE 5.0u75, 6u85, 7u72, and 8u25 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot.
CVE-2015-0407	Unspecified vulnerability in Oracle Java SE 5.0u75, 6u85, 7u72, and 8u25 allows remote attackers to affect confidentiality via unknown vectors related to Swing.
CVE-2015-0408	Unspecified vulnerability in Oracle Java SE 5.0u75, 6u85, 7u72, and 8u25 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to RMI.
CVE-2015-0410	Unspecified vulnerability in the Java SE, Java SE Embedded, JRockit component in Oracle Java SE 5.0u75, 6u85, 7u72, and 8u25; Java SE Embedded 7u71 and 8u6; and JRockit R27.8.4 and R28.3.4 allows

	remote attackers to affect availability via unknown vectors related to Security.
CVE-2015-0412	Unspecified vulnerability in Oracle Java SE 6u85, 7u72, and 8u25 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JAX-WS.
CVE-2015-0437	Unspecified vulnerability in Oracle Java SE 8u25 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot.
CVE-2015-0460	Unspecified vulnerability in Oracle Java SE 5.0u81, 6u91, 7u76, and 8u40 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot.
CVE-2015-0469	Unspecified vulnerability in Oracle Java SE 5.0u81, 6u91, 7u76, and 8u40 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.
CVE-2015-0470	Unspecified vulnerability in Oracle Java SE 8u40 allows remote attackers to affect integrity via unknown vectors related to Hotspot.
CVE-2015-0477	Unspecified vulnerability in Oracle Java SE 5.0u81, 6u91, 7u76, and 8u40 allows remote attackers to affect integrity via unknown vectors related to Beans.
CVE-2015-0478	Unspecified vulnerability in Oracle Java SE 5.0u81, 6u91, 7u76, and 8u40, and JRockit R28.3.5, allows remote attackers to affect confidentiality via vectors related to JCE.
CVE-2015-0480	Unspecified vulnerability in Oracle Java SE 5.0u81, 6u91, 7u76, and 8u40 allows remote attackers to affect integrity and availability via unknown vectors related to Tools.
CVE-2015-0488	Unspecified vulnerability in Oracle Java SE 5.0u81, 6u91, 7u76, and 8u40, and JRockit R28.3.5, allows remote attackers to affect availability via vectors related to JSSE.
CVE-2015-0562	Multiple use-after-free vulnerabilities in epan/dissectors/packet-dec-dnart.c in the DEC DNA Routing Protocol dissector in Wireshark 1.10.x before 1.10.12 and 1.12.x before 1.12.3 allow remote attackers to cause a denial of service (application crash) via a crafted packet, related to the use of packet-scope memory instead of pinfo-scope memory.
CVE-2015-0564	Buffer underflow in the ssl_decrypt_record function in epan/dissectors/packet-ssl-utils.c in Wireshark 1.10.x before 1.10.12 and 1.12.x before 1.12.3 allows remote attackers to cause a denial of service (application crash) via a crafted packet that is improperly handled during decryption of an SSL session.
CVE-2015-0837	** RESERVED **

	This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2015-0848	Heap-based buffer overflow in libwmf 0.2.8.4 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted BMP image.
CVE-2015-1158	The add_job function in scheduler/ipp.c in cupsd in CUPS before 2.0.3 performs incorrect free operations for multiple-value job-originating-host-name attributes, which allows remote attackers to trigger data corruption for reference-counted strings via a crafted (1) IPP_CREATE_JOB or (2) IPP_PRINT_JOB request, as demonstrated by replacing the configuration file and consequently executing arbitrary code.
CVE-2015-1159	Cross-site scripting (XSS) vulnerability in the cgi_puts function in cgi-bin/template.c in the template engine in CUPS before 2.0.3 allows remote attackers to inject arbitrary web script or HTML via the QUERY parameter to help/.
CVE-2015-1191	Multiple directory traversal vulnerabilities in pigz 2.3.1 allow remote attackers to write to arbitrary files via a (1) full pathname or (2) .. (dot dot) in an archive.
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-2015-1291	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-2015-1345	The bmexec_trans function in kwset.c in grep 2.19 through 2.21 allows local users to cause a denial of service (out-of-bounds heap read and crash) via crafted input when using the -F option.
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-2015-1349	named in ISC BIND 9.7.0 through 9.9.6 before 9.9.6-P2 and 9.10.x before 9.10.1-P2, when DNSSEC validation and the managed-keys feature are enabled, allows remote attackers to cause a denial of service (assertion failure and daemon exit, or daemon crash) by triggering an incorrect trust-anchor management scenario in which no key is ready for use.
CVE-2015-1351	Use-after-free vulnerability in the _zend_shared_memdup function in zend_shared_alloc.c in the OPcache extension in PHP through 5.6.7 allows remote attackers to cause a denial

	of service or possibly have unspecified other impact via unknown vectors.
CVE-2015-1352	The build_tablename function in pgsql.c in the PostgreSQL (aka pgsql) extension in PHP through 5.6.7 does not validate token extraction for table names, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted name.
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-2015-1472	The ADDW macro in stdio-common/vfscanf.c in the GNU C Library (aka glibc or libc6) before 2.21 does not properly consider data-type size during memory allocation, which allows context-dependent attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a long line containing wide characters that are improperly handled in a wscanf call.
CVE-2015-1473	The ADDW macro in stdio-common/vfscanf.c in the GNU C Library (aka glibc or libc6) before 2.21 does not properly consider data-type size during a risk-management decision for use of the alloca function, which might allow context-dependent attackers to cause a denial of service (segmentation violation) or overwrite memory locations beyond the stack boundary via a

	long line containing wide characters that are improperly handled in a wscanf call.
CVE-2015-1547	The NeXTDecode function in tif_next.c in LibTIFF allows remote attackers to cause a denial of service (uninitialized memory access) via a crafted TIFF image, as demonstrated by libtiff5.tif.
CVE-2015-1593	The stack randomization feature in the Linux kernel before 3.19.1 on 64-bit platforms uses incorrect data types for the results of bitwise left-shift operations, which makes it easier for attackers to bypass the ASLR protection mechanism by predicting the address of the top of the stack, related to the randomize_stack_top function in fs/binfmt_elf.c and the stack_maxrandom_size function in arch/x86/mm/mmap.c.
CVE-2015-1606	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2015-1781	Buffer overflow in the gethostbyname_r and other unspecified NSS functions in the GNU C Library (aka glibc or libc6) before 2.22 allows context-dependent attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS response, which triggers a call with a misaligned buffer.
CVE-2015-1789	The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.
CVE-2015-1790	The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.
CVE-2015-1791	Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a

	NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.
CVE-2015-1792	The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.
CVE-2015-1793	The X509_verify_cert function in crypto/x509/x509_vfy.c in OpenSSL 1.0.1n, 1.0.1o, 1.0.2b, and 1.0.2c does not properly process X.509 Basic Constraints cA values during identification of alternative certificate chains, which allows remote attackers to spoof a Certification Authority role and trigger unintended certificate verifications via a valid leaf certificate.
CVE-2015-1798	The symmetric-key feature in the receive function in ntp_proto.c in ntpd in NTP 4.x before 4.2.8p2 requires a correct MAC only if the MAC field has a nonzero length, which makes it easier for man-in-the-middle attackers to spoof packets by omitting the MAC.
CVE-2015-1799	The symmetric-key feature in the receive function in ntp_proto.c in ntpd in NTP 3.x and 4.x before 4.2.8p2 performs state-variable updates upon receiving certain invalid packets, which makes it easier for man-in-the-middle attackers to cause a denial of service (synchronization loss) by spoofing the source IP address of a peer.
CVE-2015-1802	The bdfReadProperties function in bitmap/bdfread.c in X.Org libXfont before 1.4.9 and 1.5.x before 1.5.1 allows remote authenticated users to cause a denial of service (out-of-bounds write and crash) or possibly execute arbitrary code via a (1) negative or (2) large property count in a BDF font file.
CVE-2015-1803	The bdfReadCharacters function in bitmap/bdfread.c in X.Org libXfont before 1.4.9 and 1.5.x before 1.5.1 does not properly handle character bitmaps it cannot read, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and crash) and possibly execute arbitrary code via a crafted BDF font file.
CVE-2015-1804	The bdfReadCharacters function in bitmap/bdfread.c in X.Org libXfont before 1.4.9 and 1.5.x before 1.5.1 does not properly perform type conversion for metrics values, which allows remote authenticated users to cause a denial of service (out-of-bounds memory access) and possibly execute arbitrary code via a crafted BDF font file.

CVE-2015-1805	The (1) pipe_read and (2) pipe_write implementations in fs/pipe.c in the Linux kernel before 3.16 do not properly consider the side effects of failed __copy_to_user_inatomic and __copy_from_user_inatomic calls, which allows local users to cause a denial of service (system crash) or possibly gain privileges via a crafted application, aka an "I/O vector array overrun."
CVE-2015-1819	The xmlreader in libxml allows remote attackers to cause a denial of service (memory consumption) via crafted XML data, related to an XML Entity Expansion (XEE) attack.
CVE-2015-1821	Heap-based buffer overflow in chrony before 1.31.1 allows remote authenticated users to cause a denial of service (chronyd crash) or possibly execute arbitrary code by configuring the (1) NTP or (2) cmdmon access with a subnet size that is indivisible by four and an address with a nonzero bit in the subnet remainder.
CVE-2015-1822	chrony before 1.31.1 does not initialize the last "next" pointer when saving unacknowledged replies to command requests, which allows remote authenticated users to cause a denial of service (uninitialized pointer dereference and daemon crash) or possibly execute arbitrary code via a large number of command requests.
CVE-2015-1853	An attacker knowing that NTP hosts A and B are peering with each other (symmetric association) can send a packet with random timestamps to host A with source address of B which will set the NTP state variables on A to the values sent by the attacker. Host A will then send on its next poll to B a packet with originate timestamp that doesn't match the transmit timestamp of B and the packet will be dropped. If the attacker does this periodically for both hosts, they won't be able to synchronize to each other. Authentication using a symmetric key can fully protect against this attack, but in implementations following the NTPv3 (RFC 1305) or NTPv4 (RFC 5905) specification the state variables were updated even when the authentication check failed and the association was not protected.
CVE-2015-1854	389 Directory Server before 1.3.3.10 allows attackers to bypass intended access restrictions and modify directory entries via a crafted ldapmodrdn call.
CVE-2015-1855	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.

CVE-2015-2154	The osi_print_cksum function in print-isoclns.c in the ethernet printer in tcpdump before 4.7.2 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted (1) length, (2) offset, or (3) base pointer checksum value.
CVE-2015-2170	The upx decoder in ClamAV before 0.98.7 allows remote attackers to cause a denial of service (crash) via a crafted file.
CVE-2015-2189	Off-by-one error in the pcapng_read function in wiretap/pcapng.c in the pcapng file parser in Wireshark 1.10.x before 1.10.13 and 1.12.x before 1.12.4 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via an invalid Interface Statistics Block (ISB) interface ID in a crafted packet.
CVE-2015-2191	Integer overflow in the dissect_tnef function in epan/dissectors/packet-tnef.c in the TNEF dissector in Wireshark 1.10.x before 1.10.13 and 1.12.x before 1.12.4 allows remote attackers to cause a denial of service (infinite loop) via a crafted length field in a packet.
CVE-2015-2221	ClamAV before 0.98.7 allows remote attackers to cause a denial of service (infinite loop) via a crafted y0da cryptor file.
CVE-2015-2222	ClamAV before 0.98.7 allows remote attackers to cause a denial of service (crash) via a crafted petite packed file.
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-2015-2296	The resolve_redirects function in sessions.py in requests 2.1.0 through 2.5.3 allows remote attackers to conduct session fixation attacks via a cookie without a host value in a redirect.
CVE-2015-2301	Use-after-free vulnerability in the phar_rename_archive function in phar_object.c in PHP before 5.5.22 and 5.6.x before 5.6.6 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted renaming of a Phar archive to the name of an existing file.

CVE-2015-2305	Integer overflow in the regcomp implementation in the Henry Spencer BSD regex library (aka rxspencer) alpha3.8.g5 on 32-bit platforms, as used in NetBSD through 6.1.5 and other products, might allow context-dependent attackers to execute arbitrary code via a large regular expression that leads to a heap-based buffer overflow.
CVE-2015-2325	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2015-2326	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2015-2331	Integer overflow in the _zip_cdir_new function in zip_dirent.c in libzip 0.11.2 and earlier, as used in the ZIP extension in PHP before 5.4.39, 5.5.x before 5.5.23, and 5.6.x before 5.6.7 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a ZIP archive that contains many entries, leading to a heap-based buffer overflow.
CVE-2015-2590	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45, and Java SE Embedded 7u75 and 8u33 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2015-4732.
CVE-2015-2601	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45, JRockit R28.3.6, and Java SE Embedded 7u75 and 8u33 allows remote attackers to affect confidentiality via vectors related to JCE.
CVE-2015-2621	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45, and Java SE Embedded 7u75 and 8u33, allows remote attackers to affect confidentiality via vectors related to JMX.
CVE-2015-2625	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45; JRockit R28.3.6; and Java SE Embedded 7u75 and 8u33 allows remote attackers to affect confidentiality via vectors related to JSSE.
CVE-2015-2628	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45, and Java SE Embedded 7u75 and 8u33 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to CORBA.

CVE-2015-2632	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45 allows remote attackers to affect confidentiality via unknown vectors related to 2D.
CVE-2015-2659	Unspecified vulnerability in Oracle Java SE 8u45 and Java SE Embedded 8u33 allows remote attackers to affect availability via unknown vectors related to Security.
CVE-2015-2665	Cross-site scripting (XSS) vulnerability in Cacti before 0.8.8d allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2015-2668	ClamAV before 0.98.7 allows remote attackers to cause a denial of service (infinite loop) via a crafted xz archive file.
CVE-2015-2694	The kdcpreauth modules in MIT Kerberos 5 (aka krb5) 1.12.x and 1.13.x before 1.13.2 do not properly track whether a client's request has been validated, which allows remote attackers to bypass an intended preauthentication requirement by providing (1) zero bytes of data or (2) an arbitrary realm name, related to plugins/preauth/otp/main.c and plugins/preauth/pkinit/pkinit_srv.c.
CVE-2015-2704	realmd allows remote attackers to inject arbitrary configurations in to sssd.conf and smb.conf via a newline character in an LDAP response.
CVE-2015-2730	Mozilla Network Security Services (NSS) before 3.19.1, as used in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and other products, does not properly perform Elliptical Curve Cryptography (ECC) multiplications, which makes it easier for remote attackers to spoof ECDSA signatures via unspecified vectors.
CVE-2015-2775	Directory traversal vulnerability in GNU Mailman before 2.1.20, when not using a static alias, allows remote attackers to execute arbitrary files via a .. (dot dot) in a list name.
CVE-2015-2783	ext/phar/phar.c in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allows remote attackers to obtain sensitive information from process memory or cause a denial of service (buffer over-read and application crash) via a crafted length value in conjunction with crafted serialized data in a phar archive, related to the phar_parse_metadata and phar_parse_pharfile functions.
CVE-2015-2808	The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using

	a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue.
CVE-2015-2925	The prepend_path function in fs/dcache.c in the Linux kernel before 4.2.4 does not properly handle rename actions inside a bind mount, which allows local users to bypass an intended container protection mechanism by renaming a directory, related to a "double-chroot attack."
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-2015-3143	cURL and libcurl 7.10.6 through 7.41.0 does not properly re-use NTLM connections, which allows remote attackers to connect as other users via an unauthenticated request, a similar issue to CVE-2014-0015.
CVE-2015-3144	The fix_hostname function in cURL and libcurl 7.37.0 through 7.41.0 does not properly calculate an index, which allows remote attackers to cause a denial of service (out-of-bounds read or write and crash) or possibly have other unspecified impact via a zero-length host name, as demonstrated by "http://:80" and ":80."
CVE-2015-3145	The sanitize_cookie_path function in cURL and libcurl 7.31.0 through 7.41.0 does not properly calculate an index, which allows remote attackers to cause a denial of service (out-of-bounds write and crash) or possibly have other unspecified impact via a cookie path containing only a double-quote character.
CVE-2015-3148	cURL and libcurl 7.10.6 through 7.41.0 do not properly re-use authenticated Negotiate connections, which allows remote attackers to connect as other users via a request.

CVE-2015-3149	The Hotspot component in OpenJDK8 as packaged in Red Hat Enterprise Linux 6 and 7 allows local users to write to arbitrary files via a symlink attack.
CVE-2015-3152	Oracle MySQL before 5.7.3, Oracle MySQL Connector/C (aka libmysqlclient) before 6.1.3, and MariaDB before 5.5.44 use the --ssl option to mean that SSL is optional, which allows man-in-the-middle attackers to spoof servers via a cleartext-downgrade attack, aka a "BACKRONYM" attack.
CVE-2015-3154	[Potential CRLF injection attacks in mail and HTTP headers]
CVE-2015-3165	Double free vulnerability in PostgreSQL before 9.0.20, 9.1.x before 9.1.16, 9.2.x before 9.2.11, 9.3.x before 9.3.7, and 9.4.x before 9.4.2 allows remote attackers to cause a denial of service (crash) by closing an SSL session at a time when the authentication timeout will expire during the session shutdown sequence.
CVE-2015-3166	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2015-3167	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2015-3183	The chunked transfer coding implementation in the Apache HTTP Server before 2.4.14 does not properly parse chunk headers, which allows remote attackers to conduct HTTP request smuggling attacks via a crafted request, related to mishandling of large chunk-size values and invalid chunk-extension characters in modules/http/http_filters.c.
CVE-2015-3184	mod_authz_svn in Apache Subversion 1.7.x before 1.7.21 and 1.8.x before 1.8.14, when using Apache httpd 2.4.x, does not properly restrict anonymous access, which allows remote anonymous users to read hidden files via the path name.
CVE-2015-3185	The ap_some_auth_required function in server/request.c in the Apache HTTP Server 2.4.x before 2.4.14 does not consider that a Require directive may be associated with an authorization setting rather than an authentication setting, which allows remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging the presence of a module that relies on the 2.2 API behavior.

CVE-2015-3187	The svn_repos_trace_node_locations function in Apache Subversion before 1.7.21 and 1.8.x before 1.8.14, when path-based authorization is used, allows remote authenticated users to obtain sensitive path information by reading the history of a node that has been moved from a hidden path.
CVE-2015-3194	crypto/rsa/rsa_ameth.c in OpenSSL 1.0.1 before 1.0.1q and 1.0.2 before 1.0.2e allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an RSA PSS ASN.1 signature that lacks a mask generation function parameter.
CVE-2015-3195	The ASN1_TFLG_COMBINE implementation in crypto/asn1/tasn_dec.c in OpenSSL before 0.9.8zh, 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1q, and 1.0.2 before 1.0.2e mishandles errors caused by malformed X509_ATTRIBUTE data, which allows remote attackers to obtain sensitive information from process memory by triggering a decoding failure in a PKCS#7 or CMS application.
CVE-2015-3196	ssl/s3_clnt.c in OpenSSL 1.0.0 before 1.0.0t, 1.0.1 before 1.0.1p, and 1.0.2 before 1.0.2d, when used for a multi-threaded client, writes the PSK identity hint to an incorrect data structure, which allows remote servers to cause a denial of service (race condition and double free) via a crafted ServerKeyExchange message.
CVE-2015-3197	ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.
CVE-2015-3202	fusermount in FUSE before 2.9.3-15 does not properly clear the environment before invoking (1) mount or (2) umount as root, which allows local users to write to arbitrary files via a crafted LIBMOUNT_MTAB environment variable that is used by mount's debugging feature.
CVE-2015-3212	Race condition in net/sctp/socket.c in the Linux kernel before 4.1.2 allows local users to cause a denial of service (list corruption and panic) via a rapid series of system calls related to sockets, as demonstrated by setsockopt calls.
CVE-2015-3216	Race condition in a certain Red Hat patch to the PRNG lock implementation in the ssleay_rand_bytes function in OpenSSL, as distributed in openssl-1.0.1e-25.el7 in Red Hat Enterprise Linux (RHEL) 7 and other products, allows remote attackers to cause a denial of service (application crash) by establishing many TLS sessions

	to a multithreaded server, leading to use of a negative value for a certain length field.
CVE-2015-3223	The ldb_wildcard_compare function in ldb_match.c in ldb before 1.1.24, as used in the AD LDAP server in Samba 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3, mishandles certain zero values, which allows remote attackers to cause a denial of service (infinite loop) via crafted packets.
CVE-2015-3230	389 Directory Server (formerly Fedora Directory Server) before 1.3.3.12 does not enforce the nsSSL3Ciphers preference when creating an sslSocket, which allows remote attackers to have unspecified impact by requesting to use a disabled cipher.
CVE-2015-3236	cURL and libcurl 7.40.0 through 7.42.1 send the HTTP Basic authentication credentials for a previous connection when reusing a reset (curl_easy_reset) connection handle to send a request to the same host name, which allows remote attackers to obtain sensitive information via unspecified vectors.
CVE-2015-3237	The smb_request_state function in cURL and libcurl 7.40.0 through 7.42.1 allows remote SMB servers to obtain sensitive information from memory or cause a denial of service (out-of-bounds read and crash) via crafted length and offset values.
CVE-2015-3238	The _unix_run_helper_binary function in the pam_unix module in Linux-PAM (aka pam) before 1.2.1, when unable to directly access passwords, allows local users to enumerate usernames or cause a denial of service (hang) via a large password.
CVE-2015-3239	Off-by-one error in the dwarf_to_unw_regnum function in include/dwarf_i.h in libunwind 1.1 allows local users to have unspecified impact via invalid dwarf opcodes.
CVE-2015-3245	Incomplete blacklist vulnerability in the chfn function in libuser before 0.56.13-8 and 0.60 before 0.60-7, as used in the userhelper program in the usermode package, allows local users to cause a denial of service (/etc/passwd corruption) via a newline character in the GECOS field.
CVE-2015-3246	libuser before 0.56.13-8 and 0.60 before 0.60-7, as used in the userhelper program in the usermode package, directly modifies /etc/passwd, which allows local users to cause a denial of service (inconsistent file state) by causing an error during the modification. NOTE: this issue can be combined with CVE-2015-3245 to gain privileges.
CVE-2015-3276	The nss_parse_ciphers function in libraries/libldap/tls_m.c in OpenLDAP does not properly parse OpenSSL-style multi-keyword mode cipher strings, which might cause a weaker than intended cipher to be

	used and allow remote attackers to have unspecified impact via unknown vectors.
CVE-2015-3329	Multiple stack-based buffer overflows in the phar_set_inode function in phar_internal.h in PHP before 5.4.40, 5.5.x before 5.5.24, and 5.6.x before 5.6.8 allow remote attackers to execute arbitrary code via a crafted length value in a (1) tar, (2) phar, or (3) ZIP archive.
CVE-2015-3331	The __driver_rfc4106_decrypt function in arch/x86/crypto/aesni-intel_glue.c in the Linux kernel before 3.19.3 does not properly determine the memory locations used for encrypted data, which allows context-dependent attackers to cause a denial of service (buffer overflow and system crash) or possibly execute arbitrary code by triggering a crypto API call, as demonstrated by use of a libkcapi test program with an AF_ALG(aead) socket.
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-2015-3405	ntp-keygen in ntp 4.2.8px before 4.2.8p2-RC2 and 4.3.x before 4.3.12 does not generate MD5 keys with sufficient entropy on big endian machines when the lowest order byte of the temp variable is between 0x20 and 0x7f and not #, which might allow remote attackers to obtain the value of generated MD5 keys via a brute force attack with the 93 possible keys.
CVE-2015-3414	SQLite before 3.8.9 does not properly implement the dequoting of collation-sequence names, which allows context-dependent attackers to cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified other impact via a crafted COLLATE clause, as demonstrated by COLLATE""""""""""" at the end of a SELECT statement.
CVE-2015-3415	The sqlite3VdbeExec function in vdbe.c in SQLite before 3.8.9 does not properly implement comparison operators, which allows context-dependent attackers to cause a denial of service (invalid free operation) or possibly have unspecified other impact via a crafted CHECK clause, as demonstrated by CHECK(0&O>O) in a CREATE TABLE statement.
CVE-2015-3416	The sqlite3VXPrintf function in printf.c in SQLite before 3.8.9 does not properly handle precision and width values during floating-point conversions, which allows context-dependent attackers to cause a denial of service (integer overflow and stack-based buffer overflow) or possibly have unspecified other impact via large integers in a crafted printf function call in a SELECT statement.
CVE-2015-3627	Libcontainer and Docker Engine before 1.6.1 opens the file-descriptor passed to the pid-1 process before performing the chroot, which allows local users to gain privileges via a symlink attack in an image.
CVE-2015-3629	Libcontainer 1.6.0, as used in Docker Engine, allows local users to escape containerization ("mount namespace breakout") and write to arbitrary file on the host system via a symlink attack in an image when respawning a container.
CVE-2015-3630	Docker Engine before 1.6.1 uses weak permissions for (1) /proc/asound, (2) /proc/timer_stats, (3) /proc/latency_stats, and (4) /proc/fs, which allows local users to modify the host, obtain sensitive information, and perform protocol downgrade attacks via a crafted image.
CVE-2015-3631	Docker Engine before 1.6.1 allows local users to set arbitrary Linux Security Modules (LSM) and docker_t

	policies via an image that allows volumes to override files in /proc.
CVE-2015-3636	The ping_unhash function in net/ipv4/ping.c in the Linux kernel before 4.0.3 does not initialize a certain list data structure during an unhash operation, which allows local users to gain privileges or cause a denial of service (use-after-free and system crash) by leveraging the ability to make a SOCK_DGRAM socket system call for the IPPROTO_ICMP or IPPROTO_ICMPV6 protocol, and then making a connect system call after a disconnect.
CVE-2015-3811	epan/dissectors/packet-wcp.c in the WCP dissector in Wireshark 1.10.x before 1.10.14 and 1.12.x before 1.12.5 improperly refers to previously processed bytes, which allows remote attackers to cause a denial of service (application crash) via a crafted packet, a different vulnerability than CVE-2015-2188.
CVE-2015-3812	Multiple memory leaks in the x11_init_protocol function in epan/dissectors/packet-x11.c in the X11 dissector in Wireshark 1.10.x before 1.10.14 and 1.12.x before 1.12.5 allow remote attackers to cause a denial of service (memory consumption) via a crafted packet.
CVE-2015-3813	The fragment_add_work function in epan/reassemble.c in the packet-reassembly feature in Wireshark 1.12.x before 1.12.5 does not properly determine the defragmentation state in a case of an insufficient snapshot length, which allows remote attackers to cause a denial of service (memory consumption) via a crafted packet.
CVE-2015-3900	RubyGems 2.0.x before 2.0.16, 2.2.x before 2.2.4, and 2.4.x before 2.4.7 does not validate the hostname when fetching gems or making API requests, which allows remote attackers to redirect requests to arbitrary domains via a crafted DNS SRV record, aka a "DNS hijack attack."
CVE-2015-3905	Buffer overflow in the set_cs_start function in t1disasm.c in t1utils before 1.39 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted font file.
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-2015-4000	The TLS protocol 1.2 and earlier, when a DHE_EXPORT ciphersuite is enabled on a server but not on a client, does not properly convey a DHE_EXPORT choice, which allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by

	DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.
CVE-2015-4020	RubyGems 2.0.x before 2.0.17, 2.2.x before 2.2.5, and 2.4.x before 2.4.8 does not validate the hostname when fetching gems or making API requests, which allows remote attackers to redirect requests to arbitrary domains via a crafted DNS SRV record with a domain that is suffixed with the original domain name, aka a "DNS hijack attack." NOTE: this vulnerability exists because to an incomplete fix for CVE-2015-3900.
CVE-2015-4021	The phar_parse_tarfile function in ext/phar/tar.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 does not verify that the first character of a filename is different from the \0 character, which allows remote attackers to cause a denial of service (integer underflow and memory corruption) via a crafted entry in a tar archive.
CVE-2015-4022	Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow.
CVE-2015-4024	Algorithmic complexity vulnerability in the multipart_buffer_headers function in main/rfc1867.c in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 allows remote attackers to cause a denial of service (CPU consumption) via crafted form data that triggers an improper order-of-growth outcome.
CVE-2015-4025	PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character in certain situations, which allows remote attackers to bypass intended extension restrictions and access files or directories with unexpected names via a crafted argument to (1) set_include_path, (2) tempnam, (3) rmdir, or (4) readlink. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.
CVE-2015-4026	The pcntl_exec implementation in PHP before 5.4.41, 5.5.x before 5.5.25, and 5.6.x before 5.6.9 truncates a pathname upon encountering a \x00 character, which might allow remote attackers to bypass intended extension restrictions and execute files with unexpected names via a crafted first argument. NOTE: this vulnerability exists because of an incomplete fix for CVE-2006-7243.
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-2015-4342	SQL injection vulnerability in Cacti before 0.8.8d allows remote attackers to execute arbitrary SQL commands via unspecified vectors involving a cdef id.
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-2015-4454	SQL injection vulnerability in the get_hash_graph_template function in lib/functions.php in Cacti before 0.8.8d allows remote attackers to execute arbitrary SQL commands via the graph_template_id parameter to graph_templates.php.
CVE-2015-4588	Heap-based buffer overflow in the DecodeImage function in libwmf 0.2.8.4 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted "run-length count" in an image in a WMF file.
CVE-2015-4620	name.c in named in ISC BIND 9.7.x through 9.9.x before 9.9.7-P1 and 9.10.x before 9.10.2-P2, when configured as a recursive resolver with DNSSEC validation, allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) by constructing crafted zone data and then making a query for a name in that zone.
CVE-2015-4634	SQL injection vulnerability in graphs.php in Cacti before 0.8.8e allows remote attackers to execute arbitrary SQL commands via the local_graph_id parameter.
CVE-2015-4642	The escapeshellarg function in ext/standard/exec.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 on Windows allows remote attackers to execute arbitrary OS commands via a crafted string to an application that accepts command-line arguments for a call to the PHP system function.
CVE-2015-4643	Integer overflow in the ftp_genlist function in ext/ftp/ftp.c in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 allows remote FTP servers to execute arbitrary code via a long reply to a LIST command, leading to a heap-based buffer overflow. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-4022.

CVE-2015-4644	The php_pgsql_meta_data function in pgsql.c in the PostgreSQL (aka pgsql) extension in PHP before 5.4.42, 5.5.x before 5.5.26, and 5.6.x before 5.6.10 does not validate token extraction for table names, which might allow remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted name. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-1352.
CVE-2015-4695	meta.h in libwmf 0.2.8.4 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WMF file.
CVE-2015-4696	Use-after-free vulnerability in libwmf 0.2.8.4 allows remote attackers to cause a denial of service (crash) via a crafted WMF file to the (1) wmf2gd or (2) wmf2eps command.
CVE-2015-4731	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45; Java SE Embedded 7u75; and Java SE Embedded 8u33 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JMX.
CVE-2015-4732	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45, and Java SE Embedded 7u75 and 8u33 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries, a different vulnerability than CVE-2015-2590.
CVE-2015-4733	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45, and Java SE Embedded 7u75 and 8u33 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to RMI.
CVE-2015-4734	Unspecified vulnerability in Oracle Java SE 6u101, 7u85 and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality via vectors related to JGSS.
CVE-2015-4748	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45; JRockit R28.3.6; and Java SE Embedded 7u75 and Embedded 8u33 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Security.
CVE-2015-4749	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45; JRockit R28.3.6; and Java SE Embedded 7u75 and 8u33 allows remote attackers to affect availability via vectors related to JNDI.
CVE-2015-4760	Unspecified vulnerability in Oracle Java SE 6u95, 7u80, and 8u45 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.
CVE-2015-4766	Unspecified vulnerability in Oracle MySQL Server 5.6.25 and earlier allows local users to affect availability

	via unknown vectors related to Server : Security : Firewall.
CVE-2015-4791	Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Security : Privileges.
CVE-2015-4792	Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition, a different vulnerability than CVE-2015-4802.
CVE-2015-4800	Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Optimizer.
CVE-2015-4802	Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition, a different vulnerability than CVE-2015-4792.
CVE-2015-4803	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60; Java SE Embedded 8u51; and JRockit R28.3.7 allows remote attackers to affect availability via vectors related to JAXP, a different vulnerability than CVE-2015-4893 and CVE-2015-4911.
CVE-2015-4805	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Serialization.
CVE-2015-4806	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality and integrity via unknown vectors related to Libraries.
CVE-2015-4807	Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier, when running on Windows, allows remote authenticated users to affect availability via unknown vectors related to Server : Query Cache.
CVE-2015-4815	Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect availability via vectors related to Server : DDL.
CVE-2015-4819	Unspecified vulnerability in Oracle MySQL Server 5.5.44 and earlier, and 5.6.25 and earlier, allows local users to affect confidentiality, integrity, and availability via unknown vectors related to Client programs.
CVE-2015-4826	Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote

	authenticated users to affect confidentiality via unknown vectors related to Server : Types.
CVE-2015-4830	Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Server : Security : Privileges.
CVE-2015-4833	Unspecified vulnerability in Oracle MySQL Server 5.6.25 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Partition.
CVE-2015-4835	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to CORBA, a different vulnerability than CVE-2015-4881.
CVE-2015-4836	Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier, and 5.6.26 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : SP.
CVE-2015-4840	Unspecified vulnerability in Oracle Java SE 7u85 and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality via unknown vectors related to 2D.
CVE-2015-4842	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality via vectors related to JAXP.
CVE-2015-4843	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.
CVE-2015-4844	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.
CVE-2015-4858	Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier, and 5.6.26 and earlier, allows remote authenticated users to affect availability via vectors related to DML, a different vulnerability than CVE-2015-4913.
CVE-2015-4860	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to RMI, a different vulnerability than CVE-2015-4883.
CVE-2015-4861	Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier, and 5.6.26 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB.

CVE-2015-4862	Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via vectors related to DML.
CVE-2015-4864	Unspecified vulnerability in Oracle MySQL Server 5.5.43 and earlier and 5.6.24 and earlier allows remote authenticated users to affect integrity via unknown vectors related to Server : Security : Privileges.
CVE-2015-4866	Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB.
CVE-2015-4868	Unspecified vulnerability in Oracle Java SE 8u60 and Java SE Embedded 8u51 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Libraries.
CVE-2015-4870	Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier, and 5.6.26 and earlier, allows remote authenticated users to affect availability via unknown vectors related to Server : Parser.
CVE-2015-4871	Unspecified vulnerability in Oracle Java SE 7u85 allows remote attackers to affect confidentiality and integrity via unknown vectors related to Libraries.
CVE-2015-4872	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60; Java SE Embedded 8u51; and JRockit R28.3.7 allows remote attackers to affect integrity via unknown vectors related to Security.
CVE-2015-4879	Unspecified vulnerability in Oracle MySQL Server 5.5.44 and earlier, and 5.6.25 and earlier, allows remote authenticated users to affect confidentiality, integrity, and availability via vectors related to DML.
CVE-2015-4881	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to CORBA, a different vulnerability than CVE-2015-4835.
CVE-2015-4882	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect availability via vectors related to CORBA.
CVE-2015-4883	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via vectors related to RMI, a different vulnerability than CVE-2015-4860.
CVE-2015-4890	Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Replication.

CVE-2015-4893	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60; Java SE Embedded 8u51; and JRockit R28.3.7 allows remote attackers to affect availability via vectors related to JAXP, a different vulnerability than CVE-2015-4803 and CVE-2015-4911.
CVE-2015-4895	Unspecified vulnerability in Oracle MySQL Server 5.6.25 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : InnoDB.
CVE-2015-4903	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality via vectors related to RMI.
CVE-2015-4904	Unspecified vulnerability in Oracle MySQL Server 5.6.25 and earlier allows remote authenticated users to affect availability via unknown vectors related to libmysqld.
CVE-2015-4905	Unspecified vulnerability in Oracle MySQL Server 5.6.23 and earlier allows remote authenticated users to affect availability via vectors related to Server : DML.
CVE-2015-4910	Unspecified vulnerability in Oracle MySQL Server 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors related to Server : Memcached.
CVE-2015-4911	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60; Java SE Embedded 8u51; and JRockit R28.3.7 allows remote attackers to affect availability via vectors related to JAXP, a different vulnerability than CVE-2015-4803 and CVE-2015-4893.
CVE-2015-4913	Unspecified vulnerability in Oracle MySQL Server 5.5.45 and earlier and 5.6.26 and earlier allows remote authenticated users to affect availability via vectors related to Server : DML, a different vulnerability than CVE-2015-4858.
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-2015-5146	ntpd in ntp before 4.2.8p3 with remote configuration enabled allows remote authenticated users with knowledge of the configuration password and access to a computer entrusted to perform remote configuration to cause a denial of service (service crash) via a NULL byte in a crafted configuration directive packet.
CVE-2015-5174	Directory traversal vulnerability in RequestUtil.java in Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.65, and 8.x before 8.0.27 allows remote authenticated users to bypass intended SecurityManager restrictions and list a parent directory via a /.. (slash dot dot) in a pathname used by a web application in a getResource, getResourceAsStream, or getResourcePaths call, as demonstrated by the $CATALINA_BASE/webapps directory.
CVE-2015-5194	The log_config_command function in ntp_parser.y in ntpd in NTP before 4.2.7p42 allows remote attackers to cause a denial of service (ntpd crash) via crafted logconfig commands.
CVE-2015-5195	ntp_openssl.m4 in ntpd in NTP before 4.2.7p112 allows remote attackers to cause a denial of service (segmentation fault) via a crafted statistics or filegen configuration command that is not enabled during compilation.

CVE-2015-5203	Double free vulnerability in the jasper_image_stop_load function in JasPer 1.900.17 allows remote attackers to cause a denial of service (crash) via a crafted JPEG 2000 image file.
CVE-2015-5219	The ULOGTOD function in ntp.d in SNTP before 4.2.7p366 does not properly perform type conversions from a precision value to a double, which allows remote attackers to cause a denial of service (infinite loop) via a crafted NTP packet.
CVE-2015-5221	Use-after-free vulnerability in the mif_process_cmpt function in libjasper/mif/mif_cod.c in the JasPer JPEG-2000 library before 1.900.2 allows remote attackers to cause a denial of service (crash) via a crafted JPEG 2000 image file.
CVE-2015-5229	The calloc function in the glibc package in Red Hat Enterprise Linux (RHEL) 6.7 and 7.2 does not properly initialize memory areas, which might allow context-dependent attackers to cause a denial of service (hang or crash) via unspecified vectors.
CVE-2015-5244	The NSSCipherSuite option with ciphersuites enabled in mod_nss before 1.0.12 allows remote attackers to bypass application restrictions.
CVE-2015-5252	vfs.c in smbd in Samba 3.x and 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3, when share names with certain substring relationships exist, allows remote attackers to bypass intended file-access restrictions via a symlink that points outside of a share.
CVE-2015-5259	Integer overflow in the read_string function in libsvn_ra_svn/marshal.c in Apache Subversion 1.9.x before 1.9.3 allows remote attackers to execute arbitrary code via an svn:// protocol string, which triggers a heap-based buffer overflow and an out-of-bounds read.
CVE-2015-5277	The get_contents function in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6) before 2.20 might allow local users to cause a denial of service (heap corruption) or gain privileges via a long line in the NSS files database.
CVE-2015-5288	The crypt function in contrib/pgcrypto in PostgreSQL before 9.0.23, 9.1.x before 9.1.19, 9.2.x before 9.2.14, 9.3.x before 9.3.10, and 9.4.x before 9.4.5 allows attackers to cause a denial of service (server crash) or read arbitrary server memory via a "too-short" salt.
CVE-2015-5289	Multiple stack-based buffer overflows in json parsing in PostgreSQL before 9.3.x before 9.3.10 and 9.4.x before 9.4.5 allow attackers to cause a denial of service (server crash) via unspecified vectors, which are not properly handled in (1) json or (2) jsonb values.

CVE-2015-5292	Memory leak in the Privilege Attribute Certificate (PAC) responder plugin (sssd_pac_plugin.so) in System Security Services Daemon (SSSD) 1.10 before 1.13.1 allows remote authenticated users to cause a denial of service (memory consumption) via a large number of logins that trigger parsing of PAC blobs during Kerberos authentication.
CVE-2015-5296	Samba 3.x and 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3 supports connections that are encrypted but unsigned, which allows man-in-the-middle attackers to conduct encrypted-to-unencrypted downgrade attacks by modifying the client-server data stream, related to clidfs.c, libsmb_server.c, and smbXcli_base.c.
CVE-2015-5299	The shadow_copy2_get_shadow_copy_data function in modules/vfs_shadow_copy2.c in Samba 3.x and 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3 does not verify that the DIRECTORY_LIST access right has been granted, which allows remote attackers to access snapshots by visiting a shadow copy directory.
CVE-2015-5300	The panic_gate check in NTP before 4.2.8p5 is only re-enabled after the first change to the system clock that was greater than 128 milliseconds by default, which allows remote attackers to set NTP to an arbitrary time when started with the -g option, or to alter the time by up to 900 seconds otherwise by responding to an unspecified number of requests from trusted sources, and leveraging a resulting denial of service (abort and restart).
CVE-2015-5312	The xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.3 does not properly prevent entity expansion, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted XML data, a different vulnerability than CVE-2014-3660.
CVE-2015-5330	ldb before 1.1.24, as used in the AD LDAP server in Samba 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3, mishandles string lengths, which allows remote attackers to obtain sensitive information from daemon heap memory by sending crafted packets and then reading (1) an error message or (2) a database value.
CVE-2015-5343	Integer overflow in util.c in mod_dav_svn in Apache Subversion 1.7.x, 1.8.x before 1.8.15, and 1.9.x before 1.9.3 allows remote authenticated users to cause a denial of service (subversion server crash or memory consumption) and possibly execute arbitrary code via a skel-encoded request body, which triggers an out-of-bounds read and heap-based buffer overflow.

CVE-2015-5345	The Mapper component in Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.68, 8.x before 8.0.30, and 9.x before 9.0.0.M2 processes redirects before considering security constraints and Filters, which allows remote attackers to determine the existence of a directory via a URL that lacks a trailing / (slash) character.
CVE-2015-5346	Session fixation vulnerability in Apache Tomcat 7.x before 7.0.66, 8.x before 8.0.30, and 9.x before 9.0.0.M2, when different session settings are used for deployments of multiple versions of the same web application, might allow remote attackers to hijack web sessions by leveraging use of a requestedSessionSSL field for an unintended request, related to CoyoteAdapter.java and Request.java.
CVE-2015-5351	The (1) Manager and (2) Host Manager applications in Apache Tomcat 7.x before 7.0.68, 8.x before 8.0.31, and 9.x before 9.0.0.M2 establish sessions and send CSRF tokens for arbitrary new requests, which allows remote attackers to bypass a CSRF protection mechanism by using a token.
CVE-2015-5352	The x11_open_helper function in channels.c in ssh in OpenSSH before 6.9, when ForwardX11Trusted mode is not used, lacks a check of the refusal deadline for X connections, which makes it easier for remote attackers to bypass intended access restrictions via a connection outside of the permitted time window.
CVE-2015-5364	The (1) udp_recvmsg and (2) udpv6_recvmsg functions in the Linux kernel before 4.0.6 do not properly consider yielding a processor, which allows remote attackers to cause a denial of service (system hang) via incorrect checksums within a UDP packet flood.
CVE-2015-5366	The (1) udp_recvmsg and (2) udpv6_recvmsg functions in the Linux kernel before 4.0.6 provide inappropriate -EAGAIN return values, which allows remote attackers to cause a denial of service (EPOLLET epoll application read outage) via an incorrect checksum in a UDP packet, a different vulnerability than CVE-2015-5364.
CVE-2015-5370	Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not properly implement the DCE-RPC layer, which allows remote attackers to perform protocol-downgrade attacks, cause a denial of service (application crash or CPU consumption), or possibly execute arbitrary code on a client system via unspecified vectors.
CVE-2015-5377	[Remote code execution vulnerability]
CVE-2015-5477	named in ISC BIND 9.x before 9.9.7-P2 and 9.10.x before 9.10.2-P3 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via TKEY queries.

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-2015-5589	The phar_convert_to_other function in ext/phar/phar_object.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 does not validate a file pointer before a close operation, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted TAR archive that is mishandled in a Phar::convertToData call.
CVE-2015-5590	Stack-based buffer overflow in the phar_fix_filepath function in ext/phar/phar.c in PHP before 5.4.43, 5.5.x before 5.5.27, and 5.6.x before 5.6.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large length value, as demonstrated by mishandling of an e-mail attachment by the imap PHP extension.
CVE-2015-5600	The kbdint_next_device function in auth2-chall.c in sshd in OpenSSH through 6.9 does not properly restrict

	the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service (CPU consumption) via a long and duplicative list in the ssh -oKbdInteractiveDevices option, as demonstrated by a modified client that provides a different password for each pam element on this list.
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-2015-5621	The snmp_pdu_parse function in snmp_api.c in net-snmp 5.7.2 and earlier does not remove the varBind variable in a netsnmp_variable_list item when parsing of the SNMP PDU fails, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted packet.
CVE-2015-5667	Cross-site scripting (XSS) vulnerability in the HTML-Scrubber module before 0.15 for Perl, when the comment feature is enabled, allows remote attackers to inject arbitrary web script or HTML via a crafted comment.
CVE-2015-5722	buffer.c in named in ISC BIND 9.x before 9.9.7-P3 and 9.10.x before 9.10.2-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) by creating a zone containing a malformed DNSSEC key and issuing a query for a name in that zone.
CVE-2015-5739	[Invalid headers are parsed as valid headers]
CVE-2015-5740	[RFC 7230 3.3.3 4 violation]
CVE-2015-5741	[RFC 7230 3.3.3 4 violation]
CVE-2015-5986	openpgpkey_61.c in named in ISC BIND 9.9.7 before 9.9.7-P3 and 9.10.x before 9.10.2-P4 allows remote attackers to cause a denial of service (REQUIRE assertion failure and daemon exit) via a crafted DNS response.
CVE-2015-6563	The monitor component in sshd in OpenSSH before 7.0 on non-OpenBSD platforms accepts extraneous username data in MONITOR_REQ_PAM_INIT_CTX requests, which allows local users to conduct impersonation attacks by leveraging any SSH login access in conjunction with control of the sshd uid to send a crafted MONITOR_REQ_PWNAM request, related to monitor.c and monitor_wrap.c.

CVE-2015-6564	Use-after-free vulnerability in the mm_answer_pam_free_ctx function in monitor.c in sshd in OpenSSH before 7.0 on non-OpenBSD platforms might allow local users to gain privileges by leveraging control of the sshd uid to send an unexpectedly early MONITOR_REQ_PAM_FREE_CTX request.
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-2015-6816	ganglia-web before 3.7.1 allows remote attackers to bypass authentication.
CVE-2015-6831	Multiple use-after-free vulnerabilities in SPL in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allow remote attackers to execute arbitrary code via vectors involving (1) ArrayObject, (2) SplObjectStorage, and (3) SplDoublyLinkedList, which are mishandled during unserialization.
CVE-2015-6832	Use-after-free vulnerability in the SPL unserialize implementation in ext/spl/spl_array.c in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to execute arbitrary code via crafted serialized data that triggers misuse of an array field.
CVE-2015-6833	Directory traversal vulnerability in the PharData class in PHP before 5.4.44, 5.5.x before 5.5.28, and 5.6.x before 5.6.12 allows remote attackers to write to arbitrary files via a .. (dot dot) in a ZIP archive entry that is mishandled during an extractTo call.
CVE-2015-6834	Multiple use-after-free vulnerabilities in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 allow remote attackers to execute arbitrary code via vectors related to (1) the Serializable interface, (2) the SplObjectStorage class, and (3) the SplDoublyLinkedList class, which are mishandled during unserialization.
CVE-2015-6835	The session deserializer in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 mishandles multiple php_var_unserialize calls, which allow remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via crafted session content.
CVE-2015-6836	The SoapClient __call method in ext/soap/soap.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13 does not properly manage headers, which allows remote attackers to execute arbitrary code via crafted serialized data that triggers a "type confusion" in the serialize_function_call function.
CVE-2015-6837	The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when libxml2 before 2.9.2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation during initial error checking, which

	allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted XML document, a different vulnerability than CVE-2015-6838.
CVE-2015-6838	The xsl_ext_function_php function in ext/xsl/xsltprocessor.c in PHP before 5.4.45, 5.5.x before 5.5.29, and 5.6.x before 5.6.13, when libxml2 before 2.9.2 is used, does not consider the possibility of a NULL valuePop return value before proceeding with a free operation after the principal argument loop, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted XML document, a different vulnerability than CVE-2015-6837.
CVE-2015-6908	The ber_get_next function in libraries/liblber/io.c in OpenLDAP 2.4.42 and earlier allows remote attackers to cause a denial of service (reachable assertion and application crash) via crafted BER data, as demonstrated by an attack against slapd.
CVE-2015-7181	The sec_asn1d_parse_leaf function in Mozilla Network Security Services (NSS) before 3.19.2.1 and 3.20.x before 3.20.1, as used in Firefox before 42.0 and Firefox ESR 38.x before 38.4 and other products, improperly restricts access to an unspecified data structure, which allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted OCTET STRING data, related to a "use-after-poison" issue.
CVE-2015-7182	Heap-based buffer overflow in the ASN.1 decoder in Mozilla Network Security Services (NSS) before 3.19.2.1 and 3.20.x before 3.20.1, as used in Firefox before 42.0 and Firefox ESR 38.x before 38.4 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted OCTET STRING data.
CVE-2015-7183	Integer overflow in the PL_ARENA_ALLOCATE implementation in Netscape Portable Runtime (NSPR) in Mozilla Network Security Services (NSS) before 3.19.2.1 and 3.20.x before 3.20.1, as used in Firefox before 42.0 and Firefox ESR 38.x before 38.4 and other products, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via unspecified vectors.
CVE-2015-7236	Use-after-free vulnerability in xprt_set_caller in rpcb_svc_com.c in rpcbind 0.2.1 and earlier allows remote attackers to cause a denial of service (daemon crash) via crafted packets, involving a PMAP_CALLIT code.
CVE-2015-7497	Heap-based buffer overflow in the xmlDictComputeFastQKey function in dict.c in libxml2

	before 2.9.3 allows context-dependent attackers to cause a denial of service via unspecified vectors.
CVE-2015-7498	Heap-based buffer overflow in the xmlParseXmlDecl function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service via unspecified vectors related to extracting errors after an encoding conversion failure.
CVE-2015-7499	Heap-based buffer overflow in the xmlGROW function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to obtain sensitive process memory information via unspecified vectors.
CVE-2015-7500	The xmlParseMisc function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service (out-of-bounds heap read) via unspecified vectors related to incorrect entities boundaries and start tags.
CVE-2015-7501	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When thecandidate has been publicized, the details for this candidate will be provided.
CVE-2015-7529	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2015-7545	The (1) git-remote-ext and (2) unspecified other remote helper programs in Git before 2.3.10, 2.4.x before 2.4.10, 2.5.x before 2.5.4, and 2.6.x before 2.6.1 do not properly restrict the allowed protocols, which might allow remote attackers to execute arbitrary code via a URL in a (a) .gitmodules file or (b) unknown other sources in a submodule.
CVE-2015-7547	Multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library in the GNU C Library (aka glibc or libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted DNS response that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family, related to performing "dual A/AAAA DNS queries" and the libnss_dns.so.2 NSS module.
CVE-2015-7551	The Fiddle::Handle implementation in ext/fiddle/handle.c in Ruby before 2.0.0-p648, 2.1 before 2.1.8, and 2.2 before 2.2.4, as distributed in Apple OS X before 10.11.4 and other products, mishandles tainting, which allows context-dependent attackers to execute arbitrary code or cause a denial of service (application

	crash) via a crafted string, related to the DL module and the libffi library. NOTE: this vulnerability exists because of a CVE-2009-5147 regression.
CVE-2015-7554	The _TIFFVGetField function in tif_dir.c in libtiff 4.0.6 allows attackers to cause a denial of service (invalid memory write and crash) or possibly have unspecified other impact via crafted field data in an extension tag in a TIFF image.
CVE-2015-7560	The SMB1 implementation in smbd in Samba 3.x and 4.x before 4.1.23, 4.2.x before 4.2.9, 4.3.x before 4.3.6, and 4.4.x before 4.4.0rc4 allows remote authenticated users to modify arbitrary ACLs by using a UNIX SMB1 call to create a symlink, and then using a non-UNIX SMB1 call to write to the ACL content.
CVE-2015-7575	Mozilla Network Security Services (NSS) before 3.20.2, as used in Mozilla Firefox before 43.0.2 and Firefox ESR 38.x before 38.5.2, does not reject MD5 signatures in Server Key Exchange messages in TLS 1.2 Handshake Protocol traffic, which makes it easier for man-in-the-middle attackers to spoof servers by triggering a collision.
CVE-2015-7613	Race condition in the IPC object implementation in the Linux kernel through 4.2.3 allows local users to gain privileges by triggering an ipc_addid call that leads to uid and gid comparisons against uninitialized data, related to msg.c, shm.c, and util.c.
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-2015-7691	The crypto_xmit function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash) via crafted packets containing particular autokey operations. NOTE: This vulnerability exists due to an incomplete fix for CVE-2014-9750.
CVE-2015-7692	The crypto_xmit function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash). NOTE:

	This vulnerability exists due to an incomplete fix for CVE-2014-9750.
CVE-2015-7700	Double-free vulnerability in the sPLT chunk structure and png.c in pngcrush before 1.7.87 allows attackers to have unspecified impact via unknown vectors.
CVE-2015-7701	Memory leak in the CRYPTO_ASSOC function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (memory consumption).
CVE-2015-7702	The crypto_xmit function in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash). NOTE: This vulnerability exists due to an incomplete fix for CVE-2014-9750.
CVE-2015-7703	The "pidfile" or "driftfile" directives in NTP ntpd 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77, when ntpd is configured to allow remote configuration, allows remote attackers with an IP address that is allowed to send configuration requests, and with knowledge of the remote configuration password to write to arbitrary files via the :config command.
CVE-2015-7704	The ntpd client in NTP 4.x before 4.2.8p4 and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service via a number of crafted "KOD" messages.
CVE-2015-7744	wolfSSL (formerly CyaSSL) before 3.6.8 does not properly handle faults associated with the Chinese Remainder Theorem (CRT) process when allowing ephemeral key exchange without low memory optimizations on a server, which makes it easier for remote attackers to obtain private RSA keys by capturing TLS handshakes, aka a Lenstra attack.
CVE-2015-7803	The phar_get_entry_data function in ext/phar/util.c in PHP before 5.5.30 and 5.6.x before 5.6.14 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a .phar file with a crafted TAR archive entry in which the Link indicator references a file that does not exist.
CVE-2015-7804	Off-by-one error in the phar_parse_zipfile function in ext/phar/zip.c in PHP before 5.5.30 and 5.6.x before 5.6.14 allows remote attackers to cause a denial of service (uninitialized pointer dereference and application crash) by including the / filename in a .zip PHAR archive.
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-2015-7852	ntpq in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to cause a denial of service (crash) via crafted mode 6 response packets.
CVE-2015-7871	Crypto-NAK packets in ntpd in NTP 4.2.x before 4.2.8p4, and 4.3.x before 4.3.77 allows remote attackers to bypass authentication.
CVE-2015-7872	The key_gc_unused_keys function in security/keys/gc.c in the Linux kernel through 4.2.6 allows local users to cause a denial of service (OOPS) via crafted keyctl commands.
CVE-2015-7941	libxml2 2.9.2 does not properly stop parsing invalid input, which allows context-dependent attackers to cause a denial of service (out-of-bounds read and libxml2 crash) via crafted XML data to the (1) xmlParseEntityDecl or (2) xmlParseConditionalSections function in parser.c, as demonstrated by non-terminated entities.
CVE-2015-7942	The xmlParseConditionalSections function in parser.c in libxml2 does not properly skip intermediary entities when it stops parsing invalid input, which allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via crafted XML data, a different vulnerability than CVE-2015-7941.
CVE-2015-7974	NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 do not verify peer associations of symmetric keys when authenticating packets, which might allow remote attackers to conduct impersonation attacks via an arbitrary trusted key, aka a "skeleton key."
CVE-2015-7977	ntpd in NTP before 4.2.8p6 and 4.3.x before 4.3.90 allows remote attackers to cause a denial of service (NULL pointer dereference) via a ntpdc reslist command.
CVE-2015-7978	NTP before 4.2.8p6 and 4.3.0 before 4.3.90 allows a remote attackers to cause a denial of service (stack exhaustion) via an ntpdc relist command, which triggers recursive traversal of the restriction list.
CVE-2015-7979	NTP before 4.2.8p6 and 4.3.x before 4.3.90 allows remote attackers to cause a denial of service (client-server association tear down) by sending broadcast packets with invalid authentication to a broadcast client.
CVE-2015-7981	The png_convert_to_rfc1123 function in png.c in libpng 1.0.x before 1.0.64, 1.2.x before 1.2.54, and 1.4.x before 1.4.17 allows remote attackers to obtain sensitive process memory information via crafted tIME chunk data in an image file, which triggers an out-of-bounds read.
CVE-2015-8000	db.c in named in ISC BIND 9.x before 9.9.8-P2 and 9.10.x before 9.10.3-P2 allows remote attackers to

	cause a denial of service (REQUIRE assertion failure and daemon exit) via a malformed class attribute.
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-2015-8138	NTP before 4.2.8p6 and 4.3.x before 4.3.90 allows remote attackers to bypass the origin timestamp validation via a packet with an origin timestamp set to zero.
CVE-2015-8139	ntpq in NTP before 4.2.8p7 allows remote attackers to obtain origin timestamps and then impersonate peers via unspecified vectors.
CVE-2015-8158	The getresponse function in ntpq in NTP versions before 4.2.8p9 and 4.3.x before 4.3.90 allows remote attackers to cause a denial of service (infinite loop) via crafted packets with incorrect values.
CVE-2015-8241	The xmlNextChar function in libxml2 2.9.2 does not properly check the state, which allows context-dependent attackers to cause a denial of service (heap-based buffer over-read and application crash) or obtain sensitive information via crafted XML data.
CVE-2015-8242	The xmlSAX2TextNode function in SAX2.c in the push interface in the HTML parser in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service (stack-based buffer over-read and application crash) or obtain sensitive information via crafted XML data.
CVE-2015-8317	The xmlParseXMLDecl function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to obtain sensitive information via an (1) unterminated encoding value or (2) incomplete XML declaration in XML data, which triggers an out-of-bounds heap read.
CVE-2015-8325	The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to

	read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.
CVE-2015-8326	The IPTables-Parse module before 1.6 for Perl allows local users to write to arbitrary files owned by the current user.
CVE-2015-8377	SQL injection vulnerability in the host_new_graphs_save function in graphs_new.php in Cacti 0.8.8f and earlier allows remote authenticated users to execute arbitrary SQL commands via crafted serialized data in the selected_graphs_array parameter in a save action.
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-2015-8472	Buffer overflow in the png_set_PLTE function in libpng before 1.0.65, 1.1.x and 1.2.x before 1.2.55, 1.3.x, 1.4.x before 1.4.18, 1.5.x before 1.5.25, and 1.6.x before 1.6.20 allows 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. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-8126.
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-2015-8557	The FontManager._get_nix_font_path function in formatters/img.py in Pygments 1.2.2 through 2.0.2 allows remote attackers to execute arbitrary commands via shell metacharacters in a font name.
CVE-2015-8560	Incomplete blacklist vulnerability in util.c in foomatic-rip in cups-filters 1.0.42 before 1.4.0 and in foomatic-filters in Foomatic 4.0.x allows remote attackers to execute arbitrary commands via a ; (semicolon) character in a print job, a different vulnerability than CVE-2015-8327.

CVE-2015-8604	SQL injection vulnerability in the host_new_graphs function in graphs_new.php in Cacti 0.8.8f and earlier allows remote authenticated users to execute arbitrary SQL commands via the cg_g parameter in a save action.
CVE-2015-8605	ISC DHCP 4.x before 4.1-ESV-R12-P1, 4.2.x, and 4.3.x before 4.3.3-P1 allows remote attackers to cause a denial of service (application crash) via an invalid length field in a UDP IPv4 packet.
CVE-2015-8629	The xdr_nullstring function in lib/kadm5/kadm_rpc_xdr.c in kadmind in MIT Kerberos 5 (aka krb5) before 1.13.4 and 1.14.x before 1.14.1 does not verify whether '\0' characters exist as expected, which allows remote authenticated users to obtain sensitive information or cause a denial of service (out-of-bounds read) via a crafted string.
CVE-2015-8630	The (1) kadm5_create_principal_3 and (2) kadm5_modify_principal functions in lib/kadm5/srv/svr_principal.c in kadmind in MIT Kerberos 5 (aka krb5) 1.12.x and 1.13.x before 1.13.4 and 1.14.x before 1.14.1 allow remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) by specifying KADM5_POLICY with a NULL policy name.
CVE-2015-8631	Multiple memory leaks in kadmin/server/server_stubs.c in kadmind in MIT Kerberos 5 (aka krb5) before 1.13.4 and 1.14.x before 1.14.1 allow remote authenticated users to cause a denial of service (memory consumption) via a request specifying a NULL principal name.
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-2015-8665	tif_getimage.c in LibTIFF 4.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) via the SamplesPerPixel tag in a TIFF image.
CVE-2015-8668	Heap-based buffer overflow in the PackBitsPreEncode function in tif_packbits.c in bmp2tiff in libtiff 4.0.6 and earlier allows remote attackers to execute arbitrary code or cause a denial of service via a large width field in a BMP image.

CVE-2015-8683	The putcontig8bitCIELab function in tif_getimage.c in LibTIFF 4.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) via a packed TIFF image.
CVE-2015-8704	apl_42.c in ISC BIND 9.x before 9.9.8-P3, 9.9.x, and 9.10.x before 9.10.3-P3 allows remote authenticated users to cause a denial of service (INSIST assertion failure and daemon exit) via a malformed Address Prefix List (APL) record.
CVE-2015-8709	** DISPUTED ** kernel/ptrace.c in the Linux kernel through 4.4.1 mishandles uid and gid mappings, which allows local users to gain privileges by establishing a user namespace, waiting for a root process to enter that namespace with an unsafe uid or gid, and then using the ptrace system call. NOTE: the vendor states "there is no kernel bug here."
CVE-2015-8767	net/sctp/sm_sideeffect.c in the Linux kernel before 4.3 does not properly manage the relationship between a lock and a socket, which allows local users to cause a denial of service (deadlock) via a crafted sctp_accept call.
CVE-2015-8776	The strftime function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly obtain sensitive information via an out-of-range time value.
CVE-2015-8777	The process_envvars function in elf/rtld.c in the GNU C Library (aka glibc or libc6) before 2.23 allows local users to bypass a pointer-guarding protection mechanism via a zero value of the LD_POINTER_GUARD environment variable.
CVE-2015-8778	Integer overflow in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via the size argument to the __hcreate_r function, which triggers out-of-bounds heap-memory access.
CVE-2015-8779	Stack-based buffer overflow in the catopen function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long catalog name.
CVE-2015-8781	tif_luv.c in libtiff allows attackers to cause a denial of service (out-of-bounds write) via an invalid number of samples per pixel in a LogL compressed TIFF image, a different vulnerability than CVE-2015-8782.
CVE-2015-8782	tif_luv.c in libtiff allows attackers to cause a denial of service (out-of-bounds writes) via a crafted TIFF image, a different vulnerability than CVE-2015-8781.

CVE-2015-8783	tif_luv.c in libtiff allows attackers to cause a denial of service (out-of-bounds reads) via a crafted TIFF image.
CVE-2015-8784	The NeXTDecode function in tif_next.c in LibTIFF allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted TIFF image, as demonstrated by libtiff5.tif.
CVE-2015-8787	The nf_nat_redirect_ipv4 function in net/netfilter/nf_nat_redirect.c in the Linux kernel before 4.4 allows remote attackers to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by sending certain IPv4 packets to an incompletely configured interface, a related issue to CVE-2003-1604.
CVE-2015-8808	The DecodeImage function in coders/gif.c in GraphicsMagick 1.3.18 allows remote attackers to cause a denial of service (uninitialized memory access) via a crafted GIF file.
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-2015-8839	Multiple race conditions in the ext4 filesystem implementation in the Linux kernel before 4.5 allow local users to cause a denial of service (disk corruption) by writing to a page that is associated with a different user's file after unsynchronized hole punching and page-fault handling.
CVE-2015-8852	Varnish 3.x before 3.0.7, when used in certain stacked installations, allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via a header line terminated by a \r (carriage return) character in conjunction with multiple Content-Length headers in an HTTP request.
CVE-2015-8863	Off-by-one error in the tokenadd function in jv_parse.c in jq allows remote attackers to cause a denial of service (crash) via a long JSON-encoded number, which triggers a heap-based buffer overflow.
CVE-2015-8865	The file_check_mem function in funcs.c in file before 5.23, as used in the Fileinfo component in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5, mishandles continuation-level jumps, which allows context-dependent attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code via a crafted magic file.
CVE-2015-8868	Heap-based buffer overflow in the ExponentialFunction::ExponentialFunction function in Poppler before 0.40.0 allows remote attackers to cause a denial of service (memory corruption and crash) or possibly execute arbitrary code via an invalid blend mode in the ExtGState dictionary in a crafted PDF document.
CVE-2015-8870	Integer overflow in tools/bmp2tiff.c in LibTIFF before 4.0.4 allows remote attackers to cause a denial of service (heap-based buffer over-read), or possibly obtain sensitive information from process memory, via crafted width and length values in RLE4 or RLE8 data in a BMP file.

CVE-2015-8874	Stack consumption vulnerability in GD in PHP before 5.6.12 allows remote attackers to cause a denial of service via a crafted imagefilltoborder call.
CVE-2015-8895	Integer overflow in coders/icon.c in ImageMagick 6.9.1-3 and later allows remote attackers to cause a denial of service (application crash) via a crafted length value, which triggers a buffer overflow.
CVE-2015-8896	Integer truncation issue in coders/pict.c in ImageMagick before 7.0.5-0 allows remote attackers to cause a denial of service (application crash) via a crafted .pict file.
CVE-2015-8897	The SpliceImage function in MagickCore/transform.c in ImageMagick before 6.9.2-4 allows remote attackers to cause a denial of service (application crash) via a crafted png file.
CVE-2015-8898	The WriteImages function in magick/constitute.c in ImageMagick before 6.9.2-4 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted image file.
CVE-2015-8916	bsdtar in libarchive before 3.2.0 returns a success code without filling the entry when the header is a "split file in multivolume RAR," which allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted rar file.
CVE-2015-8917	bsdtar in libarchive before 3.2.0 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via an invalid character in the name of a cab file.
CVE-2015-8919	The lha_read_file_extended_header function in archive_read_support_format_lha.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds heap) via a crafted (1) lzh or (2) lha file.
CVE-2015-8920	The _ar_read_header function in archive_read_support_format_ar.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds stack read) via a crafted ar file.
CVE-2015-8921	The ae_strtofflags function in archive_entry.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mtree file.
CVE-2015-8922	The read_CodersInfo function in archive_read_support_format_7zip.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted 7z file, related to the _7z_folder struct.
CVE-2015-8923	The process_extra function in libarchive before 3.2.0 uses the size field and a signed number in an offset,

	which allows remote attackers to cause a denial of service (crash) via a crafted zip file.
CVE-2015-8924	The archive_read_format_tar_read_header function in archive_read_support_format_tar.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted tar file.
CVE-2015-8925	The readline function in archive_read_support_format_mtree.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (invalid read) via a crafted mtree file, related to newline parsing.
CVE-2015-8926	The archive_read_format_rar_read_data function in archive_read_support_format_rar.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (crash) via a crafted rar archive.
CVE-2015-8928	The process_add_entry function in archive_read_support_format_mtree.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mtree file.
CVE-2015-8930	bsdtar in libarchive before 3.2.0 allows remote attackers to cause a denial of service (infinite loop) via an ISO with a directory that is a member of itself.
CVE-2015-8931	Multiple integer overflows in the (1) get_time_t_max and (2) get_time_t_min functions in archive_read_support_format_mtree.c in libarchive before 3.2.0 allow remote attackers to have unspecified impact via a crafted mtree file, which triggers undefined behavior.
CVE-2015-8932	The compress_bidder_init function in archive_read_support_filter_compress.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (crash) via a crafted tar file, which triggers an invalid left shift.
CVE-2015-8934	The copy_from_lzss_window function in archive_read_support_format_rar.c in libarchive 3.2.0 and earlier allows remote attackers to cause a denial of service (out-of-bounds heap read) via a crafted rar file.
CVE-2015-9096	Net::SMTP in Ruby before 2.4.0 is vulnerable to SMTP command injection via CRLF sequences in a RCPT TO or MAIL FROM command, as demonstrated by CRLF sequences immediately before and after a DATA substring.
CVE-2016-0402	Unspecified vulnerability in the Java SE and Java SE Embedded components in Oracle Java SE 6u105, 7u91, and 8u66 and Java SE Embedded 8u65 allows remote attackers to affect integrity via unknown vectors related to Networking.
CVE-2016-0448	Unspecified vulnerability in the Java SE and Java SE Embedded components in Oracle Java SE 6u105,

	7u91, and 8u66, and Java SE Embedded 8u65 allows remote authenticated users to affect confidentiality via vectors related to JMX.
CVE-2016-0466	Unspecified vulnerability in the Java SE, Java SE Embedded, and JRockit components in Oracle Java SE 6u105, 7u91, and 8u66; Java SE Embedded 8u65; and JRockit R28.3.8 allows remote attackers to affect availability via vectors related to JAXP.
CVE-2016-0475	Unspecified vulnerability in the Java SE, Java SE Embedded, and JRockit components in Oracle Java SE 8u66; Java SE Embedded 8u65; and JRockit R28.3.8 allows remote attackers to affect confidentiality and integrity via unknown vectors related to Libraries.
CVE-2016-0483	Unspecified vulnerability in Oracle Java SE 6u105, 7u91, and 8u66; Java SE Embedded 8u65; and JRockit R28.3.8 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to AWT. NOTE: the previous information is from the January 2016 CPU. Oracle has not commented on third-party claims that this is a heap-based buffer overflow in the readImage function, which allows remote attackers to execute arbitrary code via crafted image data.
CVE-2016-0494	Unspecified vulnerability in the Java SE and Java SE Embedded components in Oracle Java SE 6u105, 7u91, and 8u66 and Java SE Embedded 8u65 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.
CVE-2016-0502	Unspecified vulnerability in Oracle MySQL 5.5.31 and earlier and 5.6.11 and earlier allows remote authenticated users to affect availability via unknown vectors related to Optimizer.
CVE-2016-0503	Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via vectors related to DML, a different vulnerability than CVE-2016-0504.
CVE-2016-0504	Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via vectors related to DML, a different vulnerability than CVE-2016-0503.
CVE-2016-0505	Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 and MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10 allows remote authenticated users to affect availability via unknown vectors related to Options.
CVE-2016-0546	Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 and MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10 allows local users to affect confidentiality, integrity, and availability via unknown vectors related to Client. NOTE: the previous information is from

	the January 2016 CPU. Oracle has not commented on third-party claims that these are multiple buffer overflows in the mysqlshow tool that allow remote database servers to have unspecified impact via a long table or database name.
CVE-2016-0594	Unspecified vulnerability in Oracle MySQL 5.6.21 and earlier allows remote authenticated users to affect availability via vectors related to DML.
CVE-2016-0595	Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier allows remote authenticated users to affect availability via vectors related to DML.
CVE-2016-0596	Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier and 5.6.27 and earlier and MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10 allows remote authenticated users to affect availability via vectors related to DML.
CVE-2016-0597	Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 and MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10 allows remote authenticated users to affect availability via unknown vectors related to Optimizer.
CVE-2016-0598	Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 and MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10 allows remote authenticated users to affect availability via vectors related to DML.
CVE-2016-0599	Unspecified vulnerability in Oracle MySQL 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to Optimizer.
CVE-2016-0600	Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 and MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10 allows remote authenticated users to affect availability via unknown vectors related to InnoDB.
CVE-2016-0601	Unspecified vulnerability in Oracle MySQL 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to Partition.
CVE-2016-0605	Unspecified vulnerability in Oracle MySQL 5.6.26 and earlier allows remote authenticated users to affect availability via unknown vectors.
CVE-2016-0606	Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 and MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10 allows remote authenticated users to affect integrity via unknown vectors related to encryption.
CVE-2016-0607	Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to replication.

CVE-2016-0608	Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 and MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10 allows remote authenticated users to affect availability via vectors related to UDF.
CVE-2016-0609	Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier, 5.6.27 and earlier, and 5.7.9 and MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10 allows remote authenticated users to affect availability via unknown vectors related to privileges.
CVE-2016-0610	Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and MariaDB before 10.0.22 and 10.1.x before 10.1.9 allows remote authenticated users to affect availability via unknown vectors related to InnoDB.
CVE-2016-0611	Unspecified vulnerability in Oracle MySQL 5.6.27 and earlier and 5.7.9 allows remote authenticated users to affect availability via unknown vectors related to Optimizer.
CVE-2016-0616	Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier and MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10 allows remote authenticated users to affect availability via unknown vectors related to Optimizer.
CVE-2016-0636	Unspecified vulnerability in Oracle Java SE 7u97, 8u73, and 8u74 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to the Hotspot sub-component.
CVE-2016-0639	Unspecified vulnerability in Oracle MySQL 5.6.29 and earlier and 5.7.11 and earlier allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Pluggable Authentication.
CVE-2016-0640	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect integrity and availability via vectors related to DML.
CVE-2016-0641	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect confidentiality and availability via vectors related to MyISAM.
CVE-2016-0642	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect integrity and availability via vectors related to Federated.
CVE-2016-0643	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25,

	and 10.1.x before 10.1.14 allows local users to affect confidentiality via vectors related to DML.
CVE-2016-0644	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect availability via vectors related to DDL.
CVE-2016-0646	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect availability via vectors related to DML.
CVE-2016-0647	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows local users to affect availability via vectors related to FTS.
CVE-2016-0648	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows local users to affect availability via vectors related to PS.
CVE-2016-0649	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect availability via vectors related to PS.
CVE-2016-0650	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect availability via vectors related to Replication.
CVE-2016-0651	Unspecified vulnerability in Oracle MySQL 5.5.46 and earlier allows local users to affect availability via vectors related to Optimizer.
CVE-2016-0655	Unspecified vulnerability in Oracle MySQL 5.6.29 and earlier and 5.7.11 and earlier and MariaDB 10.0.x before 10.0.25 and 10.1.x before 10.1.14 allows local users to affect availability via vectors related to InnoDB.
CVE-2016-0666	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows local users to affect availability via vectors related to Security: Privileges.
CVE-2016-0686	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77 and Java SE Embedded 8u77 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Serialization.

CVE-2016-0687	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77 and Java SE Embedded 8u77 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to the Hotspot sub-component.
CVE-2016-0695	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77; Java SE Embedded 8u77; and JRockit R28.3.9 allows remote attackers to affect confidentiality via vectors related to Security.
CVE-2016-0702	The MOD_EXP_CTIME_COPY_FROM_PREBUF function in crypto/bn/bn_exp.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not properly consider cache-bank access times during modular exponentiation, which makes it easier for local users to discover RSA keys by running a crafted application on the same Intel Sandy Bridge CPU core as a victim and leveraging cache-bank conflicts, aka a "CacheBleed" attack.
CVE-2016-0703	The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.
CVE-2016-0704	An oracle protection mechanism in the get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a overwrites incorrect MASTER-KEY bytes during use of export cipher suites, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.
CVE-2016-0705	Double free vulnerability in the dsa_priv_decode function in crypto/dsa/dsa_ameth.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a malformed DSA private key.
CVE-2016-0706	Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.68, 8.x before 8.0.31, and 9.x before 9.0.0.M2 does not place org.apache.catalina.manager.StatusManagerServlet on the org/apache/catalina/core/RestrictedServlets.properties list, which allows remote authenticated users to bypass intended SecurityManager restrictions and read arbitrary HTTP requests, and consequently discover session ID values, via a crafted web application.

CVE-2016-0714	The session-persistence implementation in Apache Tomcat 6.x before 6.0.45, 7.x before 7.0.68, 8.x before 8.0.31, and 9.x before 9.0.0.M2 mishandles session attributes, which allows remote authenticated users to bypass intended SecurityManager restrictions and execute arbitrary code in a privileged context via a web application that places a crafted object in a session.
CVE-2016-0718	Expat allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a malformed input document, which triggers a buffer overflow.
CVE-2016-0723	Race condition in the tty_ioctl function in drivers/tty/tty_io.c in the Linux kernel through 4.4.1 allows local users to obtain sensitive information from kernel memory or cause a denial of service (use-after-free and system crash) by making a TIOCGETD ioctl call during processing of a TIOCSETD ioctl call.
CVE-2016-0728	The join_session_keyring function in security/keys/process_keys.c in the Linux kernel before 4.4.1 mishandles object references in a certain error case, which allows local users to gain privileges or cause a denial of service (integer overflow and use-after-free) via crafted keyctl commands.
CVE-2016-0736	In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.
CVE-2016-0741	slapd/connection.c in 389 Directory Server (formerly Fedora Directory Server) 1.3.4.x before 1.3.4.7 allows remote attackers to cause a denial of service (infinite loop and connection blocking) by leveraging an abnormally closed connection.
CVE-2016-0742	The resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 allows remote attackers to cause a denial of service (invalid pointer dereference and worker process crash) via a crafted UDP DNS response.
CVE-2016-0746	Use-after-free vulnerability in the resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 allows remote attackers to cause a denial of service (worker process crash) or possibly have unspecified other impact via a crafted DNS response related to CNAME response processing.
CVE-2016-0747	The resolver in nginx before 1.8.1 and 1.9.x before 1.9.10 does not properly limit CNAME resolution, which allows remote attackers to cause a denial of service (worker process resource consumption) via vectors related to arbitrary name resolution.

CVE-2016-0755	The ConnectionExists function in lib/url.c in libcurl before 7.47.0 does not properly re-use NTLM-authenticated proxy connections, which might allow remote attackers to authenticate as other users via a request, a similar issue to CVE-2014-0015.
CVE-2016-0758	Integer overflow in lib/asn1_decoder.c in the Linux kernel before 4.6 allows local users to gain privileges via crafted ASN.1 data.
CVE-2016-0762	The Realm implementations in Apache Tomcat versions 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 did not process the supplied password if the supplied user name did not exist. This made a timing attack possible to determine valid user names. Note that the default configuration includes the LockOutRealm which makes exploitation of this vulnerability harder.
CVE-2016-0763	The setGlobalContext method in org/apache/naming/factory/ResourceLinkFactory.java in Apache Tomcat 7.x before 7.0.68, 8.x before 8.0.31, and 9.x before 9.0.0.M3 does not consider whether ResourceLinkFactory.setGlobalContext callers are authorized, which allows remote authenticated users to bypass intended SecurityManager restrictions and read or write to arbitrary application data, or cause a denial of service (application disruption), via a web application that sets a crafted global context.
CVE-2016-0772	The smtplib library in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 does not return an error when StartTLS fails, which might allow man-in-the-middle attackers to bypass the TLS protections by leveraging a network position between the client and the registry to block the StartTLS command, aka a "StartTLS stripping attack."
CVE-2016-0773	PostgreSQL before 9.1.20, 9.2.x before 9.2.15, 9.3.x before 9.3.11, 9.4.x before 9.4.6, and 9.5.x before 9.5.1 allows remote attackers to cause a denial of service (infinite loop or buffer overflow and crash) via a large Unicode character range in a regular expression.
CVE-2016-0777	The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.
CVE-2016-0778	The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer

	overflow) or possibly have unspecified other impact by requesting many forwardings.
CVE-2016-0787	The diffie_hellman_sha256 function in kex.c in libssh2 before 1.7.0 improperly truncates secrets to 128 or 256 bits, which makes it easier for man-in-the-middle attackers to decrypt or intercept SSH sessions via unspecified vectors, aka a "bits/bytes confusion bug."
CVE-2016-0797	Multiple integer overflows in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allow remote attackers to cause a denial of service (heap memory corruption or NULL pointer dereference) or possibly have unspecified other impact via a long digit string that is mishandled by the (1) BN_dec2bn or (2) BN_hex2bn function, related to crypto/bn/bn.h and crypto/bn/bn_print.c.
CVE-2016-0799	The fmtstr function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g improperly calculates string lengths, which allows remote attackers to cause a denial of service (overflow and out-of-bounds read) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-2842.
CVE-2016-0800	The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a "DROWN" attack.
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-2016-1000110	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2016-1000111	HTTPoxy
CVE-2016-1000212	Mitigation for HTTPoxy vulnerability
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-2016-10088	The sg implementation in the Linux kernel through 4.9 does not properly restrict write operations in situations where the KERNEL_DS option is set, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device, related to block/

	bsg.c and drivers/scsi/sg.c. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-9576.
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-2016-10147	crypto/mcryptd.c in the Linux kernel before 4.8.15 allows local users to cause a denial of service (NULL pointer dereference and system crash) by using an AF_ALG socket with an incompatible algorithm, as demonstrated by mcryptd(md5).
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-2016-10158	The exif_convert_any_to_int function in ext/exif/exif.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (application crash) via crafted EXIF data that triggers an attempt to divide the minimum representable negative integer by -1.
CVE-2016-10159	Integer overflow in the phar_parse_pharfile function in ext/phar/phar.c in PHP before 5.6.30 and 7.0.x before 7.0.15 allows remote attackers to cause a denial of service (memory consumption or application crash) via a truncated manifest entry in a PHAR archive.
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-2016-10160	Off-by-one error in the phar_parse_pharfile function in ext/phar/phar.c in PHP before 5.6.30 and 7.0.x before 7.0.15 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted PHAR archive with an alias mismatch.
CVE-2016-10161	The object_common1 function in ext/standard/var_unserializer.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (buffer over-read and application crash) via crafted serialized data that is mishandled in a finish_nested_data call.
CVE-2016-10162	The php_wddx_pop_element function in ext/wddx/wddx.c in PHP 7.0.x before 7.0.15 and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an inapplicable class name in a wddxPacket XML document, leading to mishandling in a wddx_deserialize call.
CVE-2016-10167	The gdImageCreateFromGd2Ctx function in gd_gd2.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to cause a denial of service (application crash) via a crafted image file.
CVE-2016-10168	Integer overflow in gd_io.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to have unspecified impact via vectors involving the number of horizontal and vertical chunks in an image.
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-2016-10207	The Xvnc server in TigerVNC allows remote attackers to cause a denial of service (invalid memory access and crash) by terminating a TLS handshake early.
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-2016-10229	udp.c in the Linux kernel before 4.5 allows remote attackers to execute arbitrary code via UDP traffic that

	triggers an unsafe second checksum calculation during execution of a recv system call with the MSG_PEEK flag.
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-2016-10248	The jpc_tsfb_synthesize function in jpc_tsfb.c in JasPer before 1.900.9 allows remote attackers to cause a denial of service (NULL pointer dereference) via vectors involving an empty sequence.
CVE-2016-10249	Integer overflow in the jpc_dec_tiledecode function in jpc_dec.c in JasPer before 1.900.12 allows remote attackers to have unspecified impact via a crafted image file, which triggers a heap-based buffer overflow.
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-2016-10251	Integer overflow in the jpc_pi_nextcprl function in jpc_t2cod.c in JasPer before 1.900.20 allows remote attackers to have unspecified impact via a crafted file, which triggers use of an uninitialized value.
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-2016-1237	nfsd in the Linux kernel through 4.6.3 allows local users to bypass intended file-permission restrictions by setting a POSIX ACL, related to nfs2acl.c, nfs3acl.c, and nfs4acl.c.
CVE-2016-1248	vim before patch 8.0.0056 does not properly validate values for the 'filetype', 'syntax' and 'keymap' options, which may result in the execution of arbitrary code if a file with a specially crafted modeline is opened.
CVE-2016-1285	named in ISC BIND 9.x before 9.9.8-P4 and 9.10.x before 9.10.3-P4 does not properly handle DNAME records when parsing fetch reply messages, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed packet to the rndc (aka control channel) interface, related to alist.c and sexpr.c.
CVE-2016-1286	named in ISC BIND 9.x before 9.9.8-P4 and 9.10.x before 9.10.3-P4 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted signature record for a DNAME record, related to db.c and resolver.c.
CVE-2016-1494	The verify function in the RSA package for Python (Python-RSA) before 3.3 allows attackers to spoof signatures with a small public exponent via crafted signature padding, aka a BERserk attack.
CVE-2016-1521	The directrun function in directmachine.cpp in Libgraphite in Graphite 2 1.2.4, as used in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.6.1, does not validate a certain skip operation, which allows remote attackers to execute arbitrary code, obtain sensitive information, or cause a denial of service (out-of-bounds read and application crash) via a crafted Graphite smart font.
CVE-2016-1522	Code.cpp in Libgraphite in Graphite 2 1.2.4, as used in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.6.1, does not consider recursive load calls during a size check, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly execute arbitrary code via a crafted Graphite smart font.
CVE-2016-1523	The SillMap::readFace function in FeatureMap.cpp in Libgraphite in Graphite 2 1.2.4, as used in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.6.1, mishandles a return value, which allows remote attackers to cause a denial of service (missing

	initialization, NULL pointer dereference, and application crash) via a crafted Graphite smart font.
CVE-2016-1526	The TtfUtil:LocaLookup function in TtfUtil.cpp in Libgraphite in Graphite 2 1.2.4, as used in Mozilla Firefox before 43.0 and Firefox ESR 38.x before 38.6.1, incorrectly validates a size value, which allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a crafted Graphite smart font.
CVE-2016-1541	Heap-based buffer overflow in the zip_read_mac_metadata function in archive_read_support_format_zip.c in libarchive before 3.2.0 allows remote attackers to execute arbitrary code via crafted entry-size values in a ZIP archive.
CVE-2016-1548	An attacker can spoof a packet from a legitimate ntpd server with an origin timestamp that matches the peer->dst timestamp recorded for that server. After making this switch, the client in NTP 4.2.8p4 and earlier and NTPSec aa48d001683e5b791a743ec9c575aaf7d867a2b0c will reject all future legitimate server responses. It is possible to force the victim client to move time after the mode has been changed. ntpq gives no indication that the mode has been switched.
CVE-2016-1550	An exploitable vulnerability exists in the message authentication functionality of libntp in ntp 4.2.8p4 and NTPSec a5fb34b9cc89b92a8fef2f459004865c93bb7f92. An attacker can send a series of crafted messages to attempt to recover the message digest key.
CVE-2016-1577	Double free vulnerability in the jas_iccattrval_destroy function in JasPer 1.900.1 and earlier allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted ICC color profile in a JPEG 2000 image file, a different vulnerability than CVE-2014-8137.
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-2016-1762	The xmlNextChar function in libxml2 before 2.9.4 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1833	The htmlCurrentChar function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1834	Heap-based buffer overflow in the xmlStrncat function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2016-1835	Use-after-free vulnerability in the xmlSAX2AttributeNs function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2 and OS X before 10.11.5, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1836	Use-after-free vulnerability in the xmlDictComputeFastKey function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1837	Multiple use-after-free vulnerabilities in the (1) htmlPArsePubidLiteral and (2) htmlParseSystemiteral

	functions in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allow remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1838	The xmlPArserPrintFileContextInternal function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1839	The xmlDictAddString function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1840	Heap-based buffer overflow in the xmlFAParsePosCharGroup function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2016-1867	The jpc_pi_nextcprl function in JasPer 1.900.1 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG 2000 image.
CVE-2016-1903	The gdImageRotateInterpolated function in ext/gd/libgd/gd_interpolation.c in PHP before 5.5.31, 5.6.x before 5.6.17, and 7.x before 7.0.2 allows remote attackers to obtain sensitive information or cause a denial of service (out-of-bounds read and application crash) via a large bgd_color argument to the imagerotate function.
CVE-2016-1908	The client in OpenSSH before 7.2 mishandles failed cookie generation for untrusted X11 forwarding and relies on the local X11 server for access-control decisions, which allows remote X11 clients to trigger a fallback and obtain trusted X11 forwarding privileges by leveraging configuration issues on this X11 server, as demonstrated by lack of the SECURITY extension on this X11 server.
CVE-2016-1950	Heap-based buffer overflow in Mozilla Network Security Services (NSS) before 3.19.2.3 and 3.20.x and 3.21.x before 3.21.1, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to execute arbitrary code via crafted ASN.1 data in an X.509 certificate.
CVE-2016-1978	Use-after-free vulnerability in the ssl3_HandleECDHServerKeyExchange function in Mozilla Network Security Services (NSS) before 3.21,

	as used in Mozilla Firefox before 44.0, allows remote attackers to cause a denial of service or possibly have unspecified other impact by making an SSL (1) DHE or (2) ECDHE handshake at a time of high memory consumption.
CVE-2016-1979	Use-after-free vulnerability in the PK11_ImportDERPrivateKeyInfoAndReturnKey function in Mozilla Network Security Services (NSS) before 3.21.1, as used in Mozilla Firefox before 45.0, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted key data with DER encoding.
CVE-2016-1982	The remove_chunked_transfer_coding function in filters.c in Privoxy before 3.0.24 allows remote attackers to cause a denial of service (invalid read and crash) via crafted chunk-encoded content.
CVE-2016-1983	The client_host function in parsers.c in Privoxy before 3.0.24 allows remote attackers to cause a denial of service (invalid read and crash) via an empty HTTP Host header.
CVE-2016-2047	The ssl_verify_server_cert function in sql-common/client.c in MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10; Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier; and Percona Server do not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via a "/CN=" string in a field in a certificate, as demonstrated by "/OU=/CN=bar.com/CN=foo.com."
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-2016-2089	The jas_matrix_clip function in jas_seq.c in JasPer 1.900.1 allows remote attackers to cause a denial of service (invalid read and application crash) via a crafted JPEG 2000 image.
CVE-2016-2105	Integer overflow in the EVP_EncodeUpdate function in crypto/evp/encode.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a

	denial of service (heap memory corruption) via a large amount of binary data.
CVE-2016-2106	Integer overflow in the EVP_EncryptUpdate function in crypto/evp/evp_enc.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of data.
CVE-2016-2107	The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-0169.
CVE-2016-2108	The ASN.1 implementation in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption) via an ANY field in crafted serialized data, aka the "negative zero" issue.
CVE-2016-2109	The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in the ASN.1 BIO implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.
CVE-2016-2110	The NTLMSSP authentication implementation in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 allows man-in-the-middle attackers to perform protocol-downgrade attacks by modifying the client-server data stream to remove application-layer flags or encryption settings, as demonstrated by clearing the NTLMSSP_NEGOTIATE_SEAL or NTLMSSP_NEGOTIATE_SIGN option to disrupt LDAP security.
CVE-2016-2111	The NETLOGON service in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2, when a domain controller is configured, allows remote attackers to spoof the computer name of a secure channel's endpoint, and obtain sensitive session information, by running a crafted application and leveraging the ability to sniff network traffic, a related issue to CVE-2015-0005.
CVE-2016-2112	The bundled LDAP client library in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not recognize the "client ldap sasl wrapping" setting, which allows man-in-the-middle attackers to perform LDAP protocol-downgrade attacks by modifying the client-server data stream.
CVE-2016-2113	Samba 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not verify X.509 certificates from TLS

	servers, which allows man-in-the-middle attackers to spoof LDAPS and HTTPS servers and obtain sensitive information via a crafted certificate.
CVE-2016-2114	The SMB1 protocol implementation in Samba 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not recognize the "server signing = mandatory" setting, which allows man-in-the-middle attackers to spoof SMB servers by modifying the client-server data stream.
CVE-2016-2115	Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not require SMB signing within a DCERPC session over ncacn_np, which allows man-in-the-middle attackers to spoof SMB clients by modifying the client-server data stream.
CVE-2016-2116	Memory leak in the jas_iccprof_createfrombuf function in JasPer 1.900.1 and earlier allows remote attackers to cause a denial of service (memory consumption) via a crafted ICC color profile in a JPEG 2000 image file.
CVE-2016-2118	The MS-SAMR and MS-LSAD protocol implementations in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 mishandle DCERPC connections, which allows man-in-the-middle attackers to perform protocol-downgrade attacks and impersonate users by modifying the client-server data stream, aka "BADLOCK."
CVE-2016-2119	libcli/smb/smbXcli_base.c in Samba 4.x before 4.2.14, 4.3.x before 4.3.11, and 4.4.x before 4.4.5 allows man-in-the-middle attackers to bypass a client-signing protection mechanism, and consequently spoof SMB2 and SMB3 servers, via the (1) SMB2_SESSION_FLAG_IS_GUEST or (2) SMB2_SESSION_FLAG_IS_NULL flag.
CVE-2016-2125	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2016-2126	Samba version 4.0.0 up to 4.5.2 is vulnerable to privilege elevation due to incorrect handling of the PAC (Privilege Attribute Certificate) checksum. A remote, authenticated, attacker can cause the winbindd process to crash using a legitimate Kerberos ticket. A local service with access to the winbindd privileged pipe can cause winbindd to cache elevated access permissions.
CVE-2016-2161	In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.

CVE-2016-2167	The canonicalize_username function in svnserve/cyrus_auth.c in Apache Subversion before 1.8.16 and 1.9.x before 1.9.4, when Cyrus SASL authentication is used, allows remote attackers to authenticate and bypass intended access restrictions via a realm string that is a prefix of an expected repository realm string.
CVE-2016-2168	The req_check_access function in the mod_authz_svn module in the httpd server in Apache Subversion before 1.8.16 and 1.9.x before 1.9.4 allows remote authenticated users to cause a denial of service (NULL pointer dereference and crash) via a crafted header in a (1) MOVE or (2) COPY request, involving an authorization check.
CVE-2016-2177	OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.
CVE-2016-2178	The dsa_sign_setup function in crypto/dsa/dsa_ossl.c in OpenSSL through 1.0.2h does not properly ensure the use of constant-time operations, which makes it easier for local users to discover a DSA private key via a timing side-channel attack.
CVE-2016-2179	The DTLS implementation in OpenSSL before 1.1.0 does not properly restrict the lifetime of queue entries associated with unused out-of-order messages, which allows remote attackers to cause a denial of service (memory consumption) by maintaining many crafted DTLS sessions simultaneously, related to d1_lib.c, statem_dtls.c, statem_lib.c, and statem_srvr.c.
CVE-2016-2180	The TS_OBJ_print_bio function in crypto/ts/ts_lib.c in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation in OpenSSL through 1.0.2h allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted time-stamp file that is mishandled by the "openssl ts" command.
CVE-2016-2181	The Anti-Replay feature in the DTLS implementation in OpenSSL before 1.1.0 mishandles early use of a new epoch number in conjunction with a large sequence number, which allows remote attackers to cause a denial of service (false-positive packet drops) via spoofed DTLS records, related to rec_layer_d1.c and ssl3_record.c.
CVE-2016-2182	The BN_bn2dec function in crypto/bn/bn_print.c in OpenSSL before 1.1.0 does not properly validate division results, which allows remote attackers to cause a denial of service (out-of-bounds write and application

	crash) or possibly have unspecified other impact via unknown vectors.
CVE-2016-2183	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.
CVE-2016-2315	revision.c in git before 2.7.4 uses an incorrect integer data type, which allows remote attackers to execute arbitrary code via a (1) long filename or (2) many nested trees, leading to a heap-based buffer overflow.
CVE-2016-2317	Multiple buffer overflows in GraphicsMagick 1.3.23 allow remote attackers to cause a denial of service (crash) via a crafted SVG file, related to the (1) TracePoint function in magick/render.c, (2) GetToken function in magick/utility.c, and (3) GetTransformTokens function in coders/svg.c.
CVE-2016-2318	GraphicsMagick 1.3.23 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted SVG file, related to the (1) DrawImage function in magick/render.c, (2) SVGStartElement function in coders/svg.c, and (3) TraceArcPath function in magick/render.c.
CVE-2016-2324	Integer overflow in Git before 2.7.4 allows remote attackers to execute arbitrary code via a (1) long filename or (2) many nested trees, which triggers a heap-based buffer overflow.
CVE-2016-2383	The adjust_branches function in kernel/bpf/verifier.c in the Linux kernel before 4.5 does not consider the delta in the backward-jump case, which allows local users to obtain sensitive information from kernel memory by creating a packet filter and then loading crafted BPF instructions.
CVE-2016-2516	NTP before 4.2.8p7 and 4.3.x before 4.3.92, when mode7 is enabled, allows remote attackers to cause a denial of service (ntpd abort) by using the same IP address multiple times in an unconfig directive.
CVE-2016-2518	The MATCH_ASSOC function in NTP before version 4.2.8p9 and 4.3.x before 4.3.92 allows remote attackers to cause an out-of-bounds reference via an addpeer request with a large hmode value.
CVE-2016-2550	The Linux kernel before 4.5 allows local users to bypass file-descriptor limits and cause a denial of service (memory consumption) by leveraging incorrect tracking of descriptor ownership and sending each descriptor over a UNIX socket before closing it. NOTE:

	this vulnerability exists because of an incorrect fix for CVE-2013-4312.
CVE-2016-2554	Stack-based buffer overflow in ext/phar/tar.c in PHP before 5.5.32, 5.6.x before 5.6.18, and 7.x before 7.0.3 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted TAR archive.
CVE-2016-2775	ISC BIND 9.x before 9.9.9-P2, 9.10.x before 9.10.4-P2, and 9.11.x before 9.11.0b2, when lwresd or the named lwres option is enabled, allows remote attackers to cause a denial of service (daemon crash) via a long request that uses the lightweight resolver protocol.
CVE-2016-2776	buffer.c in named in ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 does not properly construct responses, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.
CVE-2016-2834	Mozilla Network Security Services (NSS) before 3.23, as used in Mozilla Firefox before 47.0, allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2016-2842	The doapr_outch function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not verify that a certain memory allocation succeeds, which allows remote attackers to cause a denial of service (out-of-bounds write or memory consumption) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-0799.
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-2016-2847	fs/pipe.c in the Linux kernel before 4.5 does not limit the amount of unread data in pipes, which allows local users to cause a denial of service (memory consumption) by creating many pipes with non-default sizes.
CVE-2016-2848	ISC BIND 9.1.0 through 9.8.4-P2 and 9.9.0 through 9.9.2-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via malformed options data in an OPT resource record.
CVE-2016-3068	Mercurial before 3.7.3 allows remote attackers to execute arbitrary code via a crafted git ext:: URL when cloning a subrepository.
CVE-2016-3069	Mercurial before 3.7.3 allows remote attackers to execute arbitrary code via a crafted name when converting a Git repository.
CVE-2016-3074	Integer signedness error in GD Graphics Library 2.1.1 (aka libgd or libgd2) allows remote attackers to cause a denial of service (crash) or potentially execute arbitrary code via crafted compressed gd2 data, which triggers a heap-based buffer overflow.
CVE-2016-3075	Stack-based buffer overflow in the nss_dns implementation of the getnetbyname function in GNU C Library (aka glibc) before 2.24 allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a long name.
CVE-2016-3092	The MultipartStream class in Apache Commons Fileupload before 1.3.2, as used in Apache Tomcat 7.x before 7.0.70, 8.x before 8.0.36, 8.5.x before 8.5.3, and 9.x before 9.0.0.M7 and other products, allows remote attackers to cause a denial of service (CPU consumption) via a long boundary string.
CVE-2016-3099	mod_ns in Red Hat Enterprise Linux Desktop 7, Red Hat Enterprise Linux HPC Node 7, Red Hat Enterprise Linux Server 7, and Red Hat Enterprise Linux Workstation 7 allows remote attackers to force the use of ciphers that were not intended to be enabled.
CVE-2016-3115	Multiple CRLF injection vulnerabilities in session.c in sshd in OpenSSH before 7.2p2 allow remote authenticated users to bypass intended shell-command restrictions via crafted X11 forwarding data, related to the (1) do_authenticated1 and (2) session_x11_req functions.
CVE-2016-3119	The process_db_args function in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in the LDAP KDB module in kadmind in MIT Kerberos 5 (aka krb5) through 1.13.4 and 1.14.x through 1.14.1 mishandles the DB argument, which allows remote authenticated users to cause a denial of service (NULL pointer dereference

	and daemon crash) via a crafted request to modify a principal.
CVE-2016-3120	The validate_as_request function in kdc_util.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.13.6 and 1.4.x before 1.14.3, when restrict_anonymous_to_tgt is enabled, uses an incorrect client data structure, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) via an S4U2Self request.
CVE-2016-3134	The netfilter subsystem in the Linux kernel through 4.5.2 does not validate certain offset fields, which allows local users to gain privileges or cause a denial of service (heap memory corruption) via an IPT_SO_SET_REPLACE setsockopt call.
CVE-2016-3135	Integer overflow in the xt_alloc_table_info function in net/netfilter/x_tables.c in the Linux kernel through 4.5.2 on 32-bit platforms allows local users to gain privileges or cause a denial of service (heap memory corruption) via an IPT_SO_SET_REPLACE setsockopt call.
CVE-2016-3156	The IPv4 implementation in the Linux kernel before 4.5.2 mishandles destruction of device objects, which allows guest OS users to cause a denial of service (host OS networking outage) by arranging for a large number of IP addresses.
CVE-2016-3157	The __switch_to function in arch/x86/kernel/process_64.c in the Linux kernel does not properly context-switch IOPL on 64-bit PV Xen guests, which allows local guest OS users to gain privileges, cause a denial of service (guest OS crash), or obtain sensitive information by leveraging I/O port access.
CVE-2016-3425	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77; Java SE Embedded 8u77; and JRockit R28.3.9 allows remote attackers to affect availability via vectors related to JAXP.
CVE-2016-3426	Unspecified vulnerability in Oracle Java SE 8u77 and Java SE Embedded 8u77 allows remote attackers to affect confidentiality via vectors related to JCE.
CVE-2016-3427	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77; Java SE Embedded 8u77; and JRockit R28.3.9 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JMX.
CVE-2016-3452	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows remote attackers to affect confidentiality via vectors related to Server: Security: Encryption.

CVE-2016-3458	Unspecified vulnerability in Oracle Java SE 6u115, 7u101, and 8u92; and Java SE Embedded 8u91 allows remote attackers to affect integrity via vectors related to CORBA.
CVE-2016-3459	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier and MariaDB 10.0.x before 10.0.25 and 10.1.x before 10.1.14 allows remote administrators to affect availability via vectors related to Server: InnoDB.
CVE-2016-3477	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows local users to affect confidentiality, integrity, and availability via vectors related to Server: Parser.
CVE-2016-3486	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote authenticated users to affect availability via vectors related to Server: FTS.
CVE-2016-3500	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-2016-3508.
CVE-2016-3501	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote authenticated users to affect availability via vectors related to Server: Optimizer.
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-2016-3521	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows remote authenticated users to affect availability via vectors related to Server: Types.
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-2016-3614	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote authenticated users to affect availability via vectors related to Server: Security: Encryption.
CVE-2016-3615	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows remote authenticated users to affect availability via vectors related to Server: DML.
CVE-2016-3627	The xmlStringGetNodeList function in tree.c in libxml2 2.9.3 and earlier, when used in recovery mode, allows context-dependent attackers to cause a denial of service (infinite recursion, stack consumption, and application crash) via a crafted XML document.
CVE-2016-3630	The binary delta decoder in Mercurial before 3.7.3 allows remote attackers to execute arbitrary code via a (1) clone, (2) push, or (3) pull command, related to (a) a list sizing rounding error and (b) short records.
CVE-2016-3632	The _TIFFVGetField function in tif_dirinfo.c in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted TIFF image.
CVE-2016-3659	SQL injection vulnerability in graph_view.php in Cacti 0.8.8.g allows remote authenticated users to execute arbitrary SQL commands via the host_group_data parameter.
CVE-2016-3672	The arch_pick_mmap_layout function in arch/x86/mm/mmap.c in the Linux kernel through 4.5.2 does not properly randomize the legacy base address, which makes it easier for local users to defeat the intended restrictions on the ADDR_NO_RANDOMIZE flag, and bypass the ASLR protection mechanism for a setuid or setgid program, by disabling stack-consumption resource limits.
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-2016-3705	The (1) xmlParserEntityCheck and (2) xmlParseAttValueComplex functions in parser.c in libxml2 2.9.3 do not properly keep track of the recursion depth, which allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a crafted XML document containing a large number of nested entity references.
CVE-2016-3714	The (1) EPHEMERAL, (2) HTTPS, (3) MVG, (4) MSL, (5) TEXT, (6) SHOW, (7) WIN, and (8) PLT coders in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allow remote attackers to execute arbitrary code via shell metacharacters in a crafted image, aka "ImageTragick."
CVE-2016-3715	The EPHEMERAL coder in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allows remote attackers to delete arbitrary files via a crafted image.
CVE-2016-3716	The MSL coder in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allows remote attackers to move arbitrary files via a crafted image.
CVE-2016-3717	The LABEL coder in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allows remote attackers to read arbitrary files via a crafted image.
CVE-2016-3718	The (1) HTTP and (2) FTP coders in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allow remote attackers to conduct server-side request forgery (SSRF) attacks via a crafted image.
CVE-2016-3945	Multiple integer overflows in the (1) cvt_by_strip and (2) cvt_by_tile functions in the tiff2rgba tool in LibTIFF 4.0.6 and earlier, when -b mode is enabled, allow remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted TIFF image, which triggers an out-of-bounds write.
CVE-2016-3959	The Verify function in crypto/dsa/dsa.go in Go before 1.5.4 and 1.6.x before 1.6.1 does not properly check parameters passed to the big integer library, which might allow remote attackers to cause a denial of service (infinite loop) via a crafted public key to a program that uses HTTPS client certificates or SSH server libraries.
CVE-2016-3961	Xen and the Linux kernel through 4.5.x do not properly suppress hugetlbfs support in x86 PV guests, which allows local PV guest OS users to cause a denial of service (guest OS crash) by attempting to access a hugetlbfs mapped area.
CVE-2016-3990	Heap-based buffer overflow in the horizontalDifference8 function in tif_pixarlog.c in LibTIFF 4.0.6 and earlier

	allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted TIFF image to tiffcp.
CVE-2016-3991	Heap-based buffer overflow in the loadImage function in the tiffcrop tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted TIFF image with zero tiles.
CVE-2016-4051	Buffer overflow in cachemgr.cgi in Squid 2.x, 3.x before 3.5.17, and 4.x before 4.0.9 might allow remote attackers to cause a denial of service or execute arbitrary code by seeding manager reports with crafted data.
CVE-2016-4052	Multiple stack-based buffer overflows in Squid 3.x before 3.5.17 and 4.x before 4.0.9 allow remote HTTP servers to cause a denial of service or execute arbitrary code via crafted Edge Side Includes (ESI) responses.
CVE-2016-4053	Squid 3.x before 3.5.17 and 4.x before 4.0.9 allow remote attackers to obtain sensitive stack layout information via crafted Edge Side Includes (ESI) responses, related to incorrect use of assert and compiler optimization.
CVE-2016-4054	Buffer overflow in Squid 3.x before 3.5.17 and 4.x before 4.0.9 allows remote attackers to execute arbitrary code via crafted Edge Side Includes (ESI) responses.
CVE-2016-4070	** DISPUTED ** Integer overflow in the php_raw_url_encode function in ext/standard/url.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to cause a denial of service (application crash) via a long string to the rawurlencode function. NOTE: the vendor says "Not sure if this qualifies as security issue (probably not)."
CVE-2016-4071	Format string vulnerability in the php_snmp_error function in ext/snmp/snmp.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to execute arbitrary code via format string specifiers in an SNMP::get call.
CVE-2016-4072	The Phar extension in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to execute arbitrary code via a crafted filename, as demonstrated by mishandling of \0 characters by the phar_analyze_path function in ext/phar/phar.c.
CVE-2016-4073	Multiple integer overflows in the mbfl_strcut function in ext/mbstring/libmbfl/mbfl/mbfilter.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted mb_strcut call.

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-2016-4300	Integer overflow in the read_SubStreamsInfo function in archive_read_support_format_7zip.c in libarchive before 3.2.1 allows remote attackers to execute arbitrary code via a 7zip file with a large number of substreams, which triggers a heap-based buffer overflow.
CVE-2016-4302	Heap-based buffer overflow in the parse_codes function in archive_read_support_format_rar.c in libarchive before 3.2.1 allows remote attackers to execute arbitrary code via a RAR file with a zero-sized dictionary.
CVE-2016-4343	The phar_make_dirstream function in ext/phar/dirstream.c in PHP before 5.6.18 and 7.x before 7.0.3 mishandles zero-size ././/@LongLink files, which allows remote attackers to cause a denial of service (uninitialized pointer dereference) or possibly have unspecified other impact via a crafted TAR archive.
CVE-2016-4356	The append_utf8_value function in the DN decoder (dn.c) in Libksba before 1.3.3 allows remote attackers to cause a denial of service (out-of-bounds read) by clearing the high bit of the byte after invalid utf-8 encoded data.
CVE-2016-4447	The xmlParseElementDecl function in parser.c in libxml2 before 2.9.4 allows context-dependent attackers to cause a denial of service (heap-based buffer underread and application crash) via a crafted file, involving xmlParseName.
CVE-2016-4448	Format string vulnerability in libxml2 before 2.9.4 allows attackers to have unspecified impact via format string specifiers in unknown vectors.
CVE-2016-4449	XML external entity (XXE) vulnerability in the xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.4, when not in validating mode, allows context-dependent attackers to read arbitrary files or cause a denial of service (resource consumption) via unspecified vectors.
CVE-2016-4450	os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.

CVE-2016-4470	The key_reject_and_link function in security/keys/key.c in the Linux kernel through 4.6.3 does not ensure that a certain data structure is initialized, which allows local users to cause a denial of service (system crash) via vectors involving a crafted keyctl request2 command.
CVE-2016-4485	The llc_cmsg_rcv function in net/llc/af_llc.c in the Linux kernel before 4.5.5 does not initialize a certain data structure, which allows attackers to obtain sensitive information from kernel stack memory by reading a message.
CVE-2016-4486	The rtnl_fill_link_ifmap function in net/core/rtnetlink.c in the Linux kernel before 4.5.5 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory by reading a Netlink message.
CVE-2016-4554	mime_header.cc in Squid before 3.5.18 allows remote attackers to bypass intended same-origin restrictions and possibly conduct cache-poisoning attacks via a crafted HTTP Host header, aka a "header smuggling" issue.
CVE-2016-4556	Double free vulnerability in Esi.cc in Squid 3.x before 3.5.18 and 4.x before 4.0.10 allows remote servers to cause a denial of service (crash) via a crafted Edge Side Includes (ESI) response.
CVE-2016-4557	The replace_map_fd_with_map_ptr function in kernel/bpf/verifier.c in the Linux kernel before 4.5.5 does not properly maintain an fd data structure, which allows local users to gain privileges or cause a denial of service (use-after-free) via crafted BPF instructions that reference an incorrect file descriptor.
CVE-2016-4558	The BPF subsystem in the Linux kernel before 4.5.5 mishandles reference counts, which allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted application on (1) a system with more than 32 Gb of memory, related to the program reference count or (2) a 1 Tb system, related to the map reference count.
CVE-2016-4565	The InfiniBand (aka IB) stack in the Linux kernel before 4.5.3 incorrectly relies on the write system call, which allows local users to cause a denial of service (kernel memory write operation) or possibly have unspecified other impact via a uAPI interface.
CVE-2016-4574	Off-by-one error in the append_utf8_value function in the DN decoder (dn.c) in Libksba before 1.3.4 allows remote attackers to cause a denial of service (out-of-bounds read) via invalid utf-8 encoded data. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-4356.
CVE-2016-4579	Libksba before 1.3.4 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via

	unspecified vectors, related to the "returned length of the object from _ksba_ber_parse_tl."
CVE-2016-4581	fs/pnode.c in the Linux kernel before 4.5.4 does not properly traverse a mount propagation tree in a certain case involving a slave mount, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted series of mount system calls.
CVE-2016-4809	The archive_read_format_cpio_read_header function in archive_read_support_format_cpio.c in libarchive before 3.2.1 allows remote attackers to cause a denial of service (application crash) via a CPIO archive with a large symlink.
CVE-2016-4861	The (1) order and (2) group methods in Zend_Db_Select in the Zend Framework before 1.12.20 might allow remote attackers to conduct SQL injection attacks by leveraging failure to remove comments from an SQL statement before validation.
CVE-2016-4913	The get_rock_ridge_filename function in fs/isofs/rock.c in the Linux kernel before 4.5.5 mishandles NM (aka alternate name) entries containing \0 characters, which allows local users to obtain sensitive information from kernel memory or possibly have unspecified other impact via a crafted isofs filesystem.
CVE-2016-4951	The tipc_nl_publ_dump function in net/tipc/socket.c in the Linux kernel through 4.6 does not verify socket existence, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a dumpit operation.
CVE-2016-4953	ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (ephemeral-association demobilization) by sending a spoofed crypto-NAK packet with incorrect authentication data at a certain time.
CVE-2016-4954	The process_packet function in ntp_proto.c in ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (peer-variable modification) by sending spoofed packets from many source IP addresses in a certain scenario, as demonstrated by triggering an incorrect leap indication.
CVE-2016-4955	ntpd in NTP 4.x before 4.2.8p8, when autokey is enabled, allows remote attackers to cause a denial of service (peer-variable clearing and association outage) by sending (1) a spoofed crypto-NAK packet or (2) a packet with an incorrect MAC value at a certain time.
CVE-2016-4956	ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (interleaved-mode transition and time change) via a spoofed broadcast packet. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-1548.

CVE-2016-4971	GNU wget before 1.18 allows remote servers to write to arbitrary files by redirecting a request from HTTP to a crafted FTP resource.
CVE-2016-4992	389 Directory Server in Red Hat Enterprise Linux Desktop 6 through 7, Red Hat Enterprise Linux HPC Node 6 through 7, Red Hat Enterprise Linux Server 6 through 7, and Red Hat Enterprise Linux Workstation 6 through 7 allows remote attackers to infer the existence of RDN component objects.
CVE-2016-4997	The compat IPT_SO_SET_REPLACE and IP6T_SO_SET_REPLACE setsockopt implementations in the netfilter subsystem in the Linux kernel before 4.6.3 allow local users to gain privileges or cause a denial of service (memory corruption) by leveraging in-container root access to provide a crafted offset value that triggers an unintended decrement.
CVE-2016-4998	The IPT_SO_SET_REPLACE setsockopt implementation in the netfilter subsystem in the Linux kernel before 4.6 allows local users to cause a denial of service (out-of-bounds read) or possibly obtain sensitive information from kernel heap memory by leveraging in-container root access to provide a crafted offset value that leads to crossing a ruleset blob boundary.
CVE-2016-5018	In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 a malicious web application was able to bypass a configured SecurityManager via a Tomcat utility method that was accessible to web applications.
CVE-2016-5093	The get_icu_value_internal function in ext/intl/locale/locale_methods.c in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7 does not ensure the presence of a '\0' character, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted locale_get_primary_language call.
CVE-2016-5094	Integer overflow in the php_html_entities function in ext/standard/html.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a large output string from the htmlspecialchars function.
CVE-2016-5095	Integer overflow in the php_escape_html_entities_ex function in ext/standard/html.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a large output string from a FILTER_SANITIZE_FULL_SPECIAL_CHARS filter_var call. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-5094.

CVE-2016-5096	Integer overflow in the fread function in ext/standard/file.c in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large integer in the second argument.
CVE-2016-5118	The OpenBlob function in blob.c in GraphicsMagick before 1.3.24 and ImageMagick allows remote attackers to execute arbitrary code via a | (pipe) character at the start of a filename.
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-2016-5195	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exploited in the wild in October 2016, aka "Dirty COW."
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-2016-5203	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-2016-5239	The gnuplot delegate functionality in ImageMagick before 6.9.4-0 and GraphicsMagick allows remote attackers to execute arbitrary commands via unspecified vectors.
CVE-2016-5240	The DrawDashPolygon function in magick/render.c in GraphicsMagick before 1.3.24 and the SVG renderer in ImageMagick allow remote attackers to cause a denial of service (infinite loop) by converting a circularly defined SVG file.
CVE-2016-5241	magick/render.c in GraphicsMagick before 1.3.24 allows remote attackers to cause a denial of service (arithmetic exception and application crash) via a crafted svg file.
CVE-2016-5243	The tipc_nl_compat_link_dump function in net/tipc/ netlink_compat.c in the Linux kernel through 4.6.3 does not properly copy a certain string, which allows local users to obtain sensitive information from kernel stack memory by reading a Netlink message.
CVE-2016-5244	The rds_inc_info_copy function in net/rds/recv.c in the Linux kernel through 4.6.3 does not initialize a certain structure member, which allows remote attackers to obtain sensitive information from kernel stack memory by reading an RDS message.
CVE-2016-5285	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2016-5320	rgb2ycbcr: command excution
CVE-2016-5385	PHP through 7.0.8 does not attempt to address RFC 3875 section 4.1.18 namespace conflicts and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, as demonstrated by (1) an application that makes a getenv('HTTP_PROXY') call or (2) a CGI configuration of PHP, aka an "httpoxy" issue.

CVE-2016-5386	The net/http package in Go through 1.6 does not attempt to address RFC 3875 section 4.1.18 namespace conflicts and therefore does not protect CGI applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect a CGI application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue.
CVE-2016-5387	The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.
CVE-2016-5388	Apache Tomcat through 8.5.4, when the CGI Servlet is enabled, follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "A mitigation is planned for future releases of Tomcat, tracked as CVE-2016-5388"; in other words, this is not a CVE ID for a vulnerability.
CVE-2016-5405	389 Directory Server in Red Hat Enterprise Linux Desktop 6 through 7, Red Hat Enterprise Linux HPC Node 6 through 7, Red Hat Enterprise Linux Server 6 through 7, and Red Hat Enterprise Linux Workstation 6 through 7 allows remote attackers to obtain user passwords.
CVE-2016-5408	Stack-based buffer overflow in the munge_other_line function in cachemgr.cgi in the squid package before 3.1.23-16.el6_8.6 in Red Hat Enterprise Linux 6 allows remote attackers to execute arbitrary code via unspecified vectors. NOTE: this vulnerability exists because of an incorrect fix for CVE-2016-4051.
CVE-2016-5416	389 Directory Server in Red Hat Enterprise Linux Desktop 6 through 7, Red Hat Enterprise Linux HPC Node 6 through 7, Red Hat Enterprise Linux Server 6 through 7, and Red Hat Enterprise Linux Workstation 6 through 7 allows remote attackers to read the default Access Control Instructions.
CVE-2016-5418	The sandboxing code in libarchive 3.2.0 and earlier mishandles hardlink archive entries of non-zero data

	size, which might allow remote attackers to write to arbitrary files via a crafted archive file.
CVE-2016-5419	curl and libcurl before 7.50.1 do not prevent TLS session resumption when the client certificate has changed, which allows remote attackers to bypass intended restrictions by resuming a session.
CVE-2016-5420	curl and libcurl before 7.50.1 do not check the client certificate when choosing the TLS connection to reuse, which might allow remote attackers to hijack the authentication of the connection by leveraging a previously created connection with a different client certificate.
CVE-2016-5421	Use-after-free vulnerability in libcurl before 7.50.1 allows attackers to control which connection is used or possibly have unspecified other impact via unknown vectors.
CVE-2016-5423	PostgreSQL before 9.1.23, 9.2.x before 9.2.18, 9.3.x before 9.3.14, 9.4.x before 9.4.9, and 9.5.x before 9.5.4 allow remote authenticated users to cause a denial of service (NULL pointer dereference and server crash), obtain sensitive memory information, or possibly execute arbitrary code via (1) a CASE expression within the test value subexpression of another CASE or (2) inlining of an SQL function that implements the equality operator used for a CASE expression involving values of different types.
CVE-2016-5424	PostgreSQL before 9.1.23, 9.2.x before 9.2.18, 9.3.x before 9.3.14, 9.4.x before 9.4.9, and 9.5.x before 9.5.4 might allow remote authenticated users with the CREATEDB or CREATEROLE role to gain superuser privileges via a (1) " (double quote), (2) \ (backslash), (3) carriage return, or (4) newline character in a (a) database or (b) role name that is mishandled during an administrative operation.
CVE-2016-5439	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Privileges.
CVE-2016-5440	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows remote administrators to affect availability via vectors related to Server: RBR.
CVE-2016-5444	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows remote attackers to affect confidentiality via vectors related to Server: Connection.
CVE-2016-5542	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows

	remote attackers to affect integrity via vectors related to Libraries.
CVE-2016-5546	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit 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 v3.0 Base Score 7.5 (Integrity impacts).
CVE-2016-5547	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. 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, JRockit. 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 v3.0 Base Score 5.3 (Availability impacts).
CVE-2016-5548	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111. 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. 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, 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 v3.0 Base Score 6.5 (Confidentiality impacts).
CVE-2016-5552	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit 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 v3.0 Base Score 5.3 (Integrity impacts).
CVE-2016-5554	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect integrity via vectors related to JMX.
CVE-2016-5573	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot, a different vulnerability than CVE-2016-5582.
CVE-2016-5582	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot, a different vulnerability than CVE-2016-5573.
CVE-2016-5597	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect confidentiality via vectors related to Networking.
CVE-2016-5636	Integer overflow in the get_data function in zipimport.c in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 allows remote attackers to have

	unspecified impact via a negative data size value, which triggers a heap-based buffer overflow.
CVE-2016-5652	An exploitable heap-based buffer overflow exists in the handling of TIFF images in LibTIFF's TIFF2PDF tool. A crafted TIFF document can lead to a heap-based buffer overflow resulting in remote code execution. Vulnerability can be triggered via a saved TIFF file delivered by other means.
CVE-2016-5696	net/ipv4/tcp_input.c in the Linux kernel before 4.7 does not properly determine the rate of challenge ACK segments, which makes it easier for remote attackers to hijack TCP sessions via a blind in-window attack.
CVE-2016-5699	CRLF injection vulnerability in the HTTPConnection.putheader function in urllib2 and urllib in CPython (aka Python) before 2.7.10 and 3.x before 3.4.4 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in a URL.
CVE-2016-5766	Integer overflow in the _gd2GetHeader function in gd_gd2.c in the GD Graphics Library (aka libgd) before 2.2.3, as used in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via crafted chunk dimensions in an image.
CVE-2016-5767	Integer overflow in the gdImageCreate function in gd.c in the GD Graphics Library (aka libgd) before 2.0.34RC1, as used in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted image dimensions.
CVE-2016-5768	Double free vulnerability in the _php_mb_regex_ereg_replace_exec function in php_mbregex.c in the mbstring extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) by leveraging a callback exception.
CVE-2016-5769	Multiple integer overflows in mcrypt.c in the mcrypt extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted length value, related to the (1) mcrypt_generic and (2) mdecrypt_generic functions.
CVE-2016-5770	Integer overflow in the SplFileObject::fread function in spl_directory.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 allows remote attackers to cause a denial of service or possibly have

	unspecified other impact via a large integer argument, a related issue to CVE-2016-5096.
CVE-2016-5771	spl_array.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data.
CVE-2016-5772	Double free vulnerability in the php_wddx_process_data function in wddx.c in the WDDX extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via crafted XML data that is mishandled in a wddx_deserialize call.
CVE-2016-5773	php_zip.c in the zip extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data containing a ZipArchive object.
CVE-2016-5844	Integer overflow in the ISO parser in libarchive before 3.2.1 allows remote attackers to cause a denial of service (application crash) via a crafted ISO file.
CVE-2016-6129	The rsa_verify_hash_ex function in rsa_verify_hash.c in LibTomCrypt, as used in OP-TEE before 2.2.0, does not validate that the message length is equal to the ASN.1 encoded data length, which makes it easier for remote attackers to forge RSA signatures or public certificates by leveraging a Bleichenbacher signature forgery attack.
CVE-2016-6233	The (1) order and (2) group methods in Zend_Db_Select in the Zend Framework before 1.12.19 might allow remote attackers to conduct SQL injection attacks via vectors related to use of the character pattern [\w]* in a regular expression.
CVE-2016-6250	Integer overflow in the ISO9660 writer in libarchive before 3.2.1 allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via vectors related to verifying filename lengths when writing an ISO9660 archive, which trigger a buffer overflow.
CVE-2016-6254	Heap-based buffer overflow in the parse_packet function in network.c in collectd before 5.4.3 and 5.x before 5.5.2 allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code via a crafted network packet.
CVE-2016-6302	The tls_decrypt_ticket function in ssl/t1_lib.c in OpenSSL before 1.1.0 does not consider the HMAC

	size during validation of the ticket length, which allows remote attackers to cause a denial of service via a ticket that is too short.
CVE-2016-6304	Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.
CVE-2016-6306	The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.
CVE-2016-6313	The mixing functions in the random number generator in Libgcrypt before 1.5.6, 1.6.x before 1.6.6, and 1.7.x before 1.7.3 and GnuPG before 1.4.21 make it easier for attackers to obtain the values of 160 bits by leveraging knowledge of the previous 4640 bits.
CVE-2016-6325	The Tomcat package on Red Hat Enterprise Linux (RHEL) 5 through 7, JBoss Web Server 3.0, and JBoss EWS 2 uses weak permissions for (1) /etc/sysconfig/tomcat and (2) /etc/tomcat/tomcat.conf, which allows local users to gain privileges by leveraging membership in the tomcat group.
CVE-2016-6329	OpenVPN, when using a 64-bit block cipher, makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTP-over-OpenVPN session using Blowfish in CBC mode, aka a "Sweet32" attack.
CVE-2016-6662	Oracle MySQL through 5.5.52, 5.6.x through 5.6.33, and 5.7.x through 5.7.15; MariaDB before 5.5.51, 10.0.x before 10.0.27, and 10.1.x before 10.1.17; and Percona Server before 5.5.51-38.1, 5.6.x before 5.6.32-78.0, and 5.7.x before 5.7.14-7 allow local users to create arbitrary configurations and bypass certain protection mechanisms by setting general_log_file to a my.cnf configuration. NOTE: this can be leveraged to execute arbitrary code with root privileges by setting malloc_lib. NOTE: the affected MySQL version information is from Oracle's October 2016 CPU. Oracle has not commented on third-party claims that the issue was silently patched in MySQL 5.5.52, 5.6.33, and 5.7.15.
CVE-2016-6663	Race condition in Oracle MySQL before 5.5.52, 5.6.x before 5.6.33, 5.7.x before 5.7.15, and 8.x before 8.0.1; MariaDB before 5.5.52, 10.0.x before 10.0.28, and 10.1.x before 10.1.18; Percona Server before 5.5.51-38.2, 5.6.x before 5.6.32-78-1, and 5.7.x before 5.7.14-8; and Percona XtraDB Cluster before 5.5.41-37.0, 5.6.x before 5.6.32-25.17, and 5.7.x before 5.7.14-26.17 allows local users with certain permissions

	to gain privileges by leveraging use of my_copystat by REPAIR TABLE to repair a MyISAM table.
CVE-2016-6794	When a SecurityManager is configured, a web application's ability to read system properties should be controlled by the SecurityManager. In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70, 6.0.0 to 6.0.45 the system property replacement feature for configuration files could be used by a malicious web application to bypass the SecurityManager and read system properties that should not be visible.
CVE-2016-6796	A malicious web application running on Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 was able to bypass a configured SecurityManager via manipulation of the configuration parameters for the JSP Servlet.
CVE-2016-6797	The ResourceLinkFactory implementation in Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 did not limit web application access to global JNDI resources to those resources explicitly linked to the web application. Therefore, it was possible for a web application to access any global JNDI resource whether an explicit ResourceLink had been configured or not.
CVE-2016-6816	The code in Apache Tomcat 9.0.0.M1 to 9.0.0.M11, 8.5.0 to 8.5.6, 8.0.0.RC1 to 8.0.38, 7.0.0 to 7.0.72, and 6.0.0 to 6.0.47 that parsed the HTTP request line permitted invalid characters. This could be exploited, in conjunction with a proxy that also permitted the invalid characters but with a different interpretation, to inject data into the HTTP response. By manipulating the HTTP response the attacker could poison a web-cache, perform an XSS attack and/or obtain sensitive information from requests other then their own.
CVE-2016-6828	The tcp_check_send_head function in include/net/tcp.h in the Linux kernel before 4.7.5 does not properly maintain certain SACK state after a failed data copy, which allows local users to cause a denial of service (tcp_xmit_retransmit_queue use-after-free and system crash) via a crafted SACK option.
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-2016-7032	sudo_noexec.so in Sudo before 1.8.15 on Linux might allow local users to bypass intended noexec command restrictions via an application that calls the (1) system or (2) popen function.
CVE-2016-7039	The IP stack in the Linux kernel through 4.8.2 allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for large crafted packets, as demonstrated by packets that contain only VLAN headers, a related issue to CVE-2016-8666.
CVE-2016-7076	noexec bypass via wordexp()
CVE-2016-7097	The filesystem implementation in the Linux kernel through 4.8.2 preserves the setgid bit during a setxattr call, which allows local users to gain group privileges by leveraging the existence of a setgid program with restrictions on execute permissions.
CVE-2016-7117	Use-after-free vulnerability in the __sys_recvmmsg function in net/socket.c in the Linux kernel before 4.5.2 allows remote attackers to execute arbitrary code via vectors involving a recvmmsg system call that is mishandled during error processing.
CVE-2016-7141	curl and libcurl before 7.50.2, when built with NSS and the libnsspem.so library is available at runtime, allow remote attackers to hijack the authentication of a TLS connection by leveraging reuse of a previously loaded client certificate from file for a connection for which no certificate has been set, a different vulnerability than CVE-2016-5420.
CVE-2016-7163	Integer overflow in the opj_pi_create_decode function in pi.c in OpenJPEG allows remote attackers to execute

	arbitrary code via a crafted JP2 file, which triggers an out-of-bounds read or write.
CVE-2016-7166	libarchive before 3.2.0 does not limit the number of recursive decompressions, which allows remote attackers to cause a denial of service (memory consumption and application crash) via a crafted gzip file.
CVE-2016-7167	Multiple integer overflows in the (1) curl_escape, (2) curl_easy_escape, (3) curl_unescape, and (4) curl_easy_unescape functions in libcurl before 7.50.3 allow attackers to have unspecified impact via a string of length 0xffffffff, which triggers a heap-based buffer overflow.
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-2016-7411	ext/standard/var_unserializer.re in PHP before 5.6.26 mishandles object-deserialization failures, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via an unserialize call that references a partially constructed object.
CVE-2016-7412	ext/mysqlnd/mysqlnd_wireprotocol.c in PHP before 5.6.26 and 7.x before 7.0.11 does not verify that a BIT field has the UNSIGNED_FLAG flag, which allows remote MySQL servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted field metadata.
CVE-2016-7413	Use-after-free vulnerability in the wddx_stack_destroy function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a wddxPacket XML document that lacks an end-tag for a recordset field element, leading to mishandling in a wddx_deserialize call.
CVE-2016-7414	The ZIP signature-verification feature in PHP before 5.6.26 and 7.x before 7.0.11 does not ensure that the uncompressed_filesize field is large enough, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via a crafted PHAR archive, related to ext/phar/util.c and ext/phar/zip.c.
CVE-2016-7416	ext/intl/msgformat/msgformat_format.c in PHP before 5.6.26 and 7.x before 7.0.11 does not properly restrict the locale length provided to the Locale class

	in the ICU library, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a MessageFormatter::formatMessage call with a long first argument.
CVE-2016-7417	ext/spl/spl_array.c in PHP before 5.6.26 and 7.x before 7.0.11 proceeds with SplArray unserialization without validating a return value and data type, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data.
CVE-2016-7418	The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service (invalid pointer access and out-of-bounds read) or possibly have unspecified other impact via an incorrect boolean element in a wddxPacket XML document, leading to mishandling in a wddx_deserialize call.
CVE-2016-7426	NTP before 4.2.8p9 rate limits responses received from the configured sources when rate limiting for all associations is enabled, which allows remote attackers to cause a denial of service (prevent responses from the sources) by sending responses with a spoofed source address.
CVE-2016-7429	NTP before 4.2.8p9 changes the peer structure to the interface it receives the response from a source, which allows remote attackers to cause a denial of service (prevent communication with a source) by sending a response for a source to an interface the source does not use.
CVE-2016-7433	NTP before 4.2.8p9 does not properly perform the initial sync calculations, which allows remote attackers to unspecified impact via unknown vectors, related to a "root distance that did not include the peer dispersion."
CVE-2016-7446	Buffer overflow in the MVG and SVG rendering code in GraphicsMagick 1.3.24 allows remote attackers to have unspecified impact via unknown vectors. Note: This vulnerability exists due to an incomplete patch for CVE-2016-2317.
CVE-2016-7447	Heap-based buffer overflow in the EscapeParenthesis function in GraphicsMagick before 1.3.25 allows remote attackers to have unspecified impact via unknown vectors.
CVE-2016-7448	The Utah RLE reader in GraphicsMagick before 1.3.25 allows remote attackers to cause a denial of service (CPU consumption or large memory allocations) via vectors involving the header information and the file size.
CVE-2016-7449	The TIFFGetField function in coders/tiff.c in GraphicsMagick 1.3.24 allows remote attackers to

	cause a denial of service (out-of-bounds heap read) via a file containing an "unterminated" string.
CVE-2016-7479	In all versions of PHP 7, during the unserialization process, resizing the 'properties' hash table of a serialized object may lead to use-after-free. A remote attacker may exploit this bug to gain arbitrary code execution.
CVE-2016-7480	The SplObjectStorage unserialize implementation in ext/spl/spl_observer.c in PHP before 7.0.12 does not verify that a key is an object, which allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access) via crafted serialized data.
CVE-2016-7545	SELinux policycoreutils allows local users to execute arbitrary commands outside of the sandbox via a crafted TIOCSTI ioctl call.
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-2016-7798	The openssl gem for Ruby uses the same initialization vector (IV) in GCM Mode (aes-*-gcm) when the IV is set before the key, which makes it easier for context-dependent attackers to bypass the encryption protection mechanism.
CVE-2016-7800	Integer underflow in the parse8BIM function in coders/meta.c in GraphicsMagick 1.3.25 and earlier allows remote attackers to cause a denial of service (application crash) via a crafted 8BIM chunk, which triggers a heap-based buffer overflow.
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-2016-7977	Ghostscript before 9.21 might allow remote attackers to bypass the SAFER mode protection mechanism and consequently read arbitrary files via the use of the .libfile operator in a crafted postscript document.
CVE-2016-7979	Ghostscript before 9.21 might allow remote attackers to bypass the SAFER mode protection mechanism and consequently execute arbitrary code by leveraging type confusion in .initialize_dsc_parser.
CVE-2016-7996	Heap-based buffer overflow in the WPG format reader in GraphicsMagick 1.3.25 and earlier allows remote attackers to have unspecified impact via a colormap with a large number of entries.
CVE-2016-7997	The WPG format reader in GraphicsMagick 1.3.25 and earlier allows remote attackers to cause a denial of service (assertion failure and crash) via vectors related to a ReferenceBlob and a NULL pointer.
CVE-2016-8318	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and 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 v3.0 Base Score 6.8 (Availability impacts).
CVE-2016-8327	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.34 and earlier and 5.7.16 and earlier. 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 v3.0 Base Score 4.4 (Availability impacts).
CVE-2016-8399	An elevation of privilege vulnerability in the kernel networking subsystem could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Moderate because it first requires compromising a privileged process and current compiler optimizations restrict access to the vulnerable code. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31349935.
CVE-2016-8602	The .sethalftone5 function in psi/zht2.c in Ghostscript before 9.21 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted Postscript document that calls .sethalftone5 with an empty operand stack.
CVE-2016-8610	Certain warning alerts are ignored if they are received. This can mean that no progress will be made if one peer continually sends those warning alerts.
CVE-2016-8615	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2016-8616	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2016-8617	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2016-8618	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2016-8619	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.

CVE-2016-8620	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2016-8621	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When thecandidate has been publicized, the details for this candidate will be provided.
CVE-2016-8622	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2016-8623	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2016-8624	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2016-8635	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2016-8645	The TCP stack in the Linux kernel before 4.8.10 mishandles skb truncation, which allows local users to cause a denial of service (system crash) via a crafted application that makes sendto system calls, related to net/ipv4/tcp_ipv4.c and net/ipv6/tcp_ipv6.c.
CVE-2016-8650	The mpi_powm function in lib/mpi/mpi-pow.c in the Linux kernel through 4.8.11 does not ensure that memory is allocated for limb data, which allows local users to cause a denial of service (stack memory corruption and panic) via an add_key system call for an RSA key with a zero exponent.
CVE-2016-8654	** RESERVED **

	This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2016-8655	Race condition in net/packet/af_packet.c in the Linux kernel through 4.8.12 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging the CAP_NET_RAW capability to change a socket version, related to the packet_set_ring and packet_setsockopt functions.
CVE-2016-8666	The IP stack in the Linux kernel before 4.6 allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for packets with tunnel stacking, as demonstrated by interleaved IPv4 headers and GRE headers, a related issue to CVE-2016-7039.
CVE-2016-8670	Integer signedness error in the dynamicGetbuf function in gd_io_dp.c in the GD Graphics Library (aka libgd) through 2.2.3, as used in PHP before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted imagecreatefromstring call.
CVE-2016-8682	The ReadSCTImage function in coders/sct.c in GraphicsMagick 1.3.25 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted SCT header.
CVE-2016-8683	The ReadPCXImage function in coders/pcx.c in GraphicsMagick 1.3.25 allows remote attackers to have unspecified impact via a crafted image, which triggers a memory allocation failure and a "file truncation error for corrupt file."
CVE-2016-8684	The MagickMalloc function in magick/memory.c in GraphicsMagick 1.3.25 allows remote attackers to have unspecified impact via a crafted image, which triggers a memory allocation failure and a "file truncation error for corrupt file."
CVE-2016-8690	The bmp_getdata function in libjasper/bmp/bmp_dec.c in JasPer before 1.900.5 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted BMP image in an imginfo command.
CVE-2016-8691	The jpc_dec_process_siz function in libjasper/jpc/jpc_dec.c in JasPer before 1.900.4 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted XRsiz value in a BMP image to the imginfo command.
CVE-2016-8692	The jpc_dec_process_siz function in libjasper/jpc/jpc_dec.c in JasPer before 1.900.4 allows remote

	attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted YRsiz value in a BMP image to the imginfo command.
CVE-2016-8693	Double free vulnerability in the mem_close function in jas_stream.c in JasPer before 1.900.10 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted BMP image to the imginfo command.
CVE-2016-8704	An integer overflow in the process_bin_append_prepend function in Memcached, which is responsible for processing multiple commands of Memcached binary protocol, can be abused to cause heap overflow and lead to remote code execution.
CVE-2016-8705	Multiple integer overflows in process_bin_update function in Memcached, which is responsible for processing multiple commands of Memcached binary protocol, can be abused to cause heap overflow and lead to remote code execution.
CVE-2016-8706	An integer overflow in process_bin_sasl_auth function in Memcached, which is responsible for authentication commands of Memcached binary protocol, can be abused to cause heap overflow and lead to remote code execution.
CVE-2016-8734	Unrestricted XML entity expansion in mod_dontdothat and Subversion clients using http(s)://
CVE-2016-8735	Remote code execution is possible with Apache Tomcat before 6.0.48, 7.x before 7.0.73, 8.x before 8.0.39, 8.5.x before 8.5.7, and 9.x before 9.0.0.M12 if JmxRemoteLifecycleListener is used and an attacker can reach JMX ports. The issue exists because this listener wasn't updated for consistency with the CVE-2016-3427 Oracle patch that affected credential types.
CVE-2016-8743	Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.
CVE-2016-8745	A bug in the error handling of the send file code for the NIO HTTP connector in Apache Tomcat 9.0.0.M1 to 9.0.0.M13, 8.5.0 to 8.5.8, 8.0.0.RC1 to 8.0.39, 7.0.0 to 7.0.73 and 6.0.16 to 6.0.48 resulted in the current Processor object being added to the Processor cache multiple times. This in turn meant that the same Processor could be used for concurrent requests. Sharing a Processor can result in information leakage

	between requests including, not not limited to, session ID and the response body. The bug was first noticed in 8.5.x onwards where it appears the refactoring of the Connector code for 8.5.x onwards made it more likely that the bug was observed. Initially it was thought that the 8.5.x refactoring introduced the bug but further investigation has shown that the bug is present in all currently supported Tomcat versions.
CVE-2016-8864	named in ISC BIND 9.x before 9.9.9-P4, 9.10.x before 9.10.4-P4, and 9.11.x before 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a DNAME record in the answer section of a response to a recursive query, related to db.c and resolver.c.
CVE-2016-8883	The jpc_dec_tiledecode function in jpc_dec.c in JasPer before 1.900.8 allows remote attackers to cause a denial of service (assertion failure) via a crafted file.
CVE-2016-8884	The bmp_getdata function in libjasper/bmp/bmp_dec.c in JasPer 1.900.5 allows remote attackers to cause a denial of service (NULL pointer dereference) by calling the imginfo command with a crafted BMP image. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8690.
CVE-2016-8885	The bmp_getdata function in libjasper/bmp/bmp_dec.c in JasPer before 1.900.9 allows remote attackers to cause a denial of service (NULL pointer dereference) by calling the imginfo command with a crafted BMP image.
CVE-2016-9083	drivers/vfio/pci/vfio_pci.c in the Linux kernel through 4.8.11 allows local users to bypass integer overflow checks, and cause a denial of service (memory corruption) or have unspecified other impact, by leveraging access to a vfio PCI device file for a VFIO_DEVICE_SET_IRQS ioctl call, aka a "state machine confusion bug."
CVE-2016-9084	drivers/vfio/pci/vfio_pci_intrs.c in the Linux kernel through 4.8.11 misuses the kzalloc function, which allows local users to cause a denial of service (integer overflow) or have unspecified other impact by leveraging access to a vfio PCI device file.
CVE-2016-9137	Use-after-free vulnerability in the CURLFile implementation in ext/curl/curl_file.c in PHP before 5.6.27 and 7.x before 7.0.12 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that is mishandled during __wakeup processing.
CVE-2016-9147	named in ISC BIND 9.9.9-P4, 9.9.9-S6, 9.10.4-P4, and 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a response containing an inconsistency among the DNSSEC-related RRsets.

CVE-2016-9262	Multiple integer overflows in the (1) jas_realloc function in base/jas_malloc.c and (2) mem_resize function in base/jas_stream.c in JasPer before 1.900.22 allow remote attackers to cause a denial of service via a crafted image, which triggers use after free vulnerabilities.
CVE-2016-9310	The control mode (mode 6) functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to set or unset traps via a crafted control mode packet.
CVE-2016-9311	ntpd in NTP before 4.2.8p9, when the trap service is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted packet.
CVE-2016-9387	Integer overflow in the jpc_dec_process_siz function in libjasper/jpc/jpc_dec.c in JasPer before 1.900.13 allows remote attackers to have unspecified impact via a crafted file, which triggers an assertion failure.
CVE-2016-9388	The ras_getcmap function in ras_dec.c in JasPer before 1.900.14 allows remote attackers to cause a denial of service (assertion failure) via a crafted image file.
CVE-2016-9389	The jpc_irct and jpc_iict functions in jpc_mct.c in JasPer before 1.900.14 allow remote attackers to cause a denial of service (assertion failure).
CVE-2016-9390	The jas_seq2d_create function in jas_seq.c in JasPer before 1.900.14 allows remote attackers to cause a denial of service (assertion failure) via a crafted image file.
CVE-2016-9391	The jpc_bitstream_getbits function in jpc_bs.c in JasPer before 2.0.10 allows remote attackers to cause a denial of service (assertion failure) via a very large integer.
CVE-2016-9392	The calcstepsizes function in jpc_dec.c in JasPer before 1.900.17 allows remote attackers to cause a denial of service (assertion failure) via a crafted file.
CVE-2016-9393	The jpc_pi_nextrpcl function in jpc_t2cod.c in JasPer before 1.900.17 allows remote attackers to cause a denial of service (assertion failure) via a crafted file.
CVE-2016-9394	The jas_seq2d_create function in jas_seq.c in JasPer before 1.900.17 allows remote attackers to cause a denial of service (assertion failure) via a crafted file.
CVE-2016-9533	tif_pixarlog.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in heap allocated buffers. Reported as MSVR 35094, aka "PixarLog horizontalDifference heap-buffer-overflow."
CVE-2016-9534	tif_write.c in libtiff 4.0.6 has an issue in the error code path of TIFFFlushData1() that didn't reset the tif_rawcc and tif_rawcp members. Reported as MSVR 35095, aka "TIFFFlushData1 heap-buffer-overflow."

CVE-2016-9535	tif_predict.h and tif_predict.c in libtiff 4.0.6 have assertions that can lead to assertion failures in debug mode, or buffer overflows in release mode, when dealing with unusual tile size like YCbCr with subsampling. Reported as MSVR 35105, aka "Predictor heap-buffer-overflow."
CVE-2016-9536	tools/tiff2pdf.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in heap allocated buffers in t2p_process_jpeg_strip(). Reported as MSVR 35098, aka "t2p_process_jpeg_strip heap-buffer-overflow."
CVE-2016-9537	tools/tiffcrop.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in buffers. Reported as MSVR 35093, MSVR 35096, and MSVR 35097.
CVE-2016-9540	tools/tiffcp.c in libtiff 4.0.6 has an out-of-bounds write on tiled images with odd tile width versus image width. Reported as MSVR 35103, aka "cpStripToTile heap-buffer-overflow."
CVE-2016-9560	Stack-based buffer overflow in the jpc_tsfb_getbands2 function in jpc_tsfb.c in JasPer before 1.900.30 allows remote attackers to have unspecified impact via a crafted image.
CVE-2016-9566	base/logging.c in Nagios Core before 4.2.4 allows local users with access to an account in the nagios group to gain root privileges via a symlink attack on the log file. NOTE: this can be leveraged by remote attackers using CVE-2016-9565.
CVE-2016-9576	The blk_rq_map_user_iov function in block/blk-map.c in the Linux kernel before 4.8.14 does not properly restrict the type of iterator, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device.
CVE-2016-9583	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2016-9586	libcurl's implementation of the printf() functions triggers a buffer overflow when doing a large floating point output. The bug occurs when the conversion outputs more than 255 bytes. This flaw does not exist in the command line tool.
CVE-2016-9591	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.

CVE-2016-9600	Null Pointer Dereference due to missing check for UNKNOWN color space in JP2 encoder
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	Private property access in V8
CVE-2016-9675	openjpeg: A heap-based buffer overflow flaw was found in the patch for CVE-2013-6045. A crafted j2k image could cause the application to crash, or potentially execute arbitrary code.
CVE-2016-9793	The sock_setsockopt function in net/core/sock.c in the Linux kernel before 4.8.14 mishandles negative values of sk_sndbuf and sk_rcvbuf, which allows local users to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact by leveraging the CAP_NET_ADMIN capability for a crafted setsockopt system call with the (1) SO_SNDBUFFORCE or (2) SO_RCVBUFFORCE option.
CVE-2016-9806	Race condition in the netlink_dump function in net/netlink/af_netlink.c in the Linux kernel before 4.6.3 allows local users to cause a denial of service (double free) or possibly have unspecified other impact via a crafted application that makes sendmsg system calls, leading to a free operation associated with a new dump that started earlier than anticipated.
CVE-2016-9830	The MagickRealloc function in memory.c in Graphicsmagick 1.3.25 allows remote attackers to cause a denial of service (crash) via large dimensions in a jpeg image.
CVE-2016-9933	Stack consumption vulnerability in the gdImageFillToBorder function in gd.c in the GD Graphics Library (aka libgd) before 2.2.2, as used in PHP before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (segmentation violation) via a crafted imagefilltoborder call that triggers use of a negative color value.
CVE-2016-9934	ext/wddx/wddx.c in PHP before 5.6.28 and 7.x before 7.0.13 allows remote attackers to cause a denial of service (NULL pointer dereference) via crafted serialized data in a wddxPacket XML document, as demonstrated by a PDORow string.
CVE-2016-9935	The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.29 and 7.x before 7.0.14 allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly

	have unspecified other impact via an empty boolean element in a wddxPacket XML document.
CVE-2016-9936	The unserialize implementation in ext/standard/var.c in PHP 7.x before 7.0.14 allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted serialized data. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-6834.
CVE-2016-9962	RunC allowed additional container processes via 'runc exec' to be ptraced by the pid 1 of the container. This allows the main processes of the container, if running as root, to gain access to file-descriptors of these new processes during the initialization and can lead to container escapes or modification of runC state before the process is fully placed inside the container.
CVE-2016-9963	Exim before 4.87.1 might allow remote attackers to obtain the private DKIM signing key via vectors related to log files and bounce messages.
CVE-2017-0553	An elevation of privilege vulnerability in libnl could enable a local malicious application to execute arbitrary code within the context of the Wi-Fi service. This issue is rated as Moderate because it first requires compromising a privileged process and is mitigated by current platform configurations. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32342065. NOTE: this issue also exists in the upstream libnl before 3.3.0 library.
CVE-2017-0898	Ruby before 2.4.2, 2.3.5, and 2.2.8 is vulnerable to a malicious format string which contains a precious specifier (*) with a huge minus value. Such situation can lead to a buffer overrun, resulting in a heap memory corruption or an information disclosure from the heap.
CVE-2017-0899	RubyGems version 2.6.12 and earlier is vulnerable to maliciously crafted gem specifications that include terminal escape characters. Printing the gem specification would execute terminal escape sequences.
CVE-2017-0900	RubyGems version 2.6.12 and earlier is vulnerable to maliciously crafted gem specifications to cause a denial of service attack against RubyGems clients who have issued a `query` command.
CVE-2017-0901	RubyGems version 2.6.12 and earlier fails to validate specification names, allowing a maliciously crafted gem to potentially overwrite any file on the filesystem.
CVE-2017-0902	RubyGems version 2.6.12 and earlier is vulnerable to a DNS hijacking vulnerability that allows a MITM attacker to force the RubyGems client to download and install gems from a server that the attacker controls.

CVE-2017-1000061	xmlsec 1.2.23 and before is vulnerable to XML External Entity Expansion when parsing crafted input documents, resulting in possible information disclosure or denial of service
CVE-2017-1000115	Mercurial prior to version 4.3 is vulnerable to a missing symlink check that can malicious repositories to modify files outside the repository
CVE-2017-1000116	Mercurial prior to 4.3 did not adequately sanitize hostnames passed to ssh, leading to possible shell-injection attacks.
CVE-2017-1000117	A malicious third-party can give a crafted"ssh://..."URL to an unsuspecting victim, and an attempt to visit the URL can result in anyprogram that exists on the victim's machine being executed. Such a URL could be placed in the .gitmodules file of a malicious project, and anunsuspecting victim could be tricked into running"git clone --recurse-submodules"to trigger the vulnerability.
CVE-2017-1000249	An issue in file() was introduced in commit 9611f31313a93aa036389c5f3b15eea53510d4d1 (Oct 2016) lets an attacker overwrite a fixed 20 bytes stack buffer with a specially crafted .notes section in an ELF binary. This was fixed in commit 35c94dc6acc418f1ad7f6241a6680e5327495793 (Aug 2017).
CVE-2017-1000253	Linux distributions that have not patched their long-term kernels with https://git.kernel.org/linus/a87938b2e246b81b4fb713edb371a9fa3c5c3c86 (committed on April 14, 2015). This kernel vulnerability was fixed in April 2015 by commit a87938b2e246b81b4fb713edb371a9fa3c5c3c86 (backported to Linux 3.10.77 in May 2015), but it was not recognized as a security threat. With CONFIG_ARCH_BINFMT_ELF_RANDOMIZE_PIE enabled, and a normal top-down address allocation strategy, load_elf_binary() will attempt to map a PIE binary into an address range immediately below mm->mmap_base. Unfortunately, load_elf_ binary() does not take account of the need to allocate sufficient space for the entire binary which means that, while the first PT_LOAD segment is mapped below mm->mmap_base, the subsequent PT_LOAD segment(s) end up being mapped above mm->mmap_base into the are that is supposed to be the "gap" between the stack and the binary.
CVE-2017-1000366	glibc contains a vulnerability that allows specially crafted LD_LIBRARY_PATH values to manipulate the heap/stack, causing them to alias, potentially resulting in arbitrary code execution. Please note that additional hardening changes have been made to glibc to prevent

	manipulation of stack and heap memory but these issues are not directly exploitable, as such they have not been given a CVE. This affects glibc 2.25 and earlier.
CVE-2017-1000367	Todd Miller's sudo version 1.8.20 and earlier is vulnerable to an input validation (embedded spaces) in the get_process_ttyname() function resulting in information disclosure and command execution.
CVE-2017-1000368	Todd Miller's sudo version 1.8.20p1 and earlier is vulnerable to an input validation (embedded newlines) in the get_process_ttyname() function resulting in information disclosure and command execution.
CVE-2017-1000381	The c-ares function `ares_parse_naptr_reply()`, which is used for parsing NAPTR responses, could be triggered to read memory outside of the given input buffer if the passed in DNS response packet was crafted in a particular way.
CVE-2017-10053	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. 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, JRockit. Note: 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-2017-10067	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131. 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 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 3.0 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-2017-10074	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. 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-2017-10081	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. 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. 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 3.0 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-2017-10087	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. 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 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 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10089	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: ImageIO). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131. Easily exploitable 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 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10090	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u141 and 8u131; Java SE Embedded: 8u131. 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 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 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10096	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. 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 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 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10101	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. 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 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 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10102	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols 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 takeover 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 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).
CVE-2017-10107	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. 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 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 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10108	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. 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, JRockit. Note: 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-2017-10109	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. 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, JRockit. 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 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-2017-10110	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131. Easily exploitable 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 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10111	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). The supported version that is affected is Java SE: 8u131; Java SE Embedded: 8u131. 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 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 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10115	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JCE). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: 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 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-2017-10116	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: 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 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-2017-10135	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JCE). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: 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 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2017-10193	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. 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 3.0 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-2017-10198	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, Java SE Embedded, JRockit, 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, JRockit accessible data. Note: 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 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-2017-10243	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JAX-WS). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded, JRockit accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit.

	Note: 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 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).
CVE-2017-10784	The Basic authentication code in WEBrick library in Ruby before 2.2.8, 2.3.x before 2.3.5, and 2.4.x through 2.4.1 allows remote attackers to inject terminal emulator escape sequences into its log and possibly execute arbitrary commands via a crafted user name.
CVE-2017-10970	Cross-site scripting (XSS) vulnerability in link.php in Cacti 1.1.12 allows remote anonymous users to inject arbitrary web script or HTML via the id parameter, related to the die_html_input_error function in lib/html_validate.php.
CVE-2017-10978	An FR-GV-201 issue in FreeRADIUS 2.x before 2.2.10 and 3.x before 3.0.15 allows "Read / write overflow in make_secret()" and a denial of service.
CVE-2017-10979	An FR-GV-202 issue in FreeRADIUS 2.x before 2.2.10 allows "Write overflow in rad_coalesce()" - this allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code.
CVE-2017-10980	An FR-GV-203 issue in FreeRADIUS 2.x before 2.2.10 allows "DHCP - Memory leak in decode_tlv()" and a denial of service.
CVE-2017-10981	An FR-GV-204 issue in FreeRADIUS 2.x before 2.2.10 allows "DHCP - Memory leak in fr_dhcp_decode()" and a denial of service.
CVE-2017-10982	An FR-GV-205 issue in FreeRADIUS 2.x before 2.2.10 allows "DHCP - Buffer over-read in fr_dhcp_decode_options()" and a denial of service.
CVE-2017-10983	An FR-GV-206 issue in FreeRADIUS 2.x before 2.2.10 and 3.x before 3.0.15 allows "DHCP - Read overflow when decoding option 63" and a denial of service.
CVE-2017-11403	The ReadMNGImage function in coders/png.c in GraphicsMagick 1.3.26 has an out-of-order CloseBlob call, resulting in a use-after-free via a crafted file.
CVE-2017-12065	spikekill.php in Cacti before 1.1.16 might allow remote attackers to execute arbitrary code via the avgnan, outlier-start, or outlier-end parameter.
CVE-2017-12066	Cross-site scripting (XSS) vulnerability in aggregate_graphs.php in Cacti before 1.1.16 allows remote authenticated users to inject arbitrary web script or HTML via specially crafted HTTP Referer headers, related to the $cancel_url variable. NOTE:

	this vulnerability exists because of an incomplete fix (lack of the htmlspecialchars ENT_QUOTES flag) for CVE-2017-11163.
CVE-2017-12150	SMB1/2/3 connections may not require signing where they should
CVE-2017-12151	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2017-12163	Server memory information leak over SMB1
CVE-2017-12927	A cross-site scripting vulnerability exists in Cacti 1.1.17 in the method parameter in spikekill.php.
CVE-2017-12978	lib/html.php in Cacti before 1.1.18 has XSS via the title field of an external link added by an authenticated user.
CVE-2017-14033	The decode method in the OpenSSL::ASN1 module in Ruby before 2.2.8, 2.3.x before 2.3.5, and 2.4.x through 2.4.1 allows attackers to cause a denial of service (interpreter crash) via a crafted string.
CVE-2017-14064	Ruby through 2.2.7, 2.3.x through 2.3.4, and 2.4.x through 2.4.1 can expose arbitrary memory during a JSON.generate call. The issues lies in using strdup in ext/json/ext/generator/generator.c, which will stop after encountering a '\0' byte, returning a pointer to a string of length zero, which is not the length stored in space_len.
CVE-2017-14482	GNU Emacs before 25.3 allows remote attackers to execute arbitrary code via email with crafted "Content-Type: text/enriched" data containing an x-display XML element that specifies execution of shell commands, related to an unsafe text/enriched extension in lisp/textmodes/enriched.el, and unsafe Gnus support for enriched and richtext inline MIME objects in lisp/gnus/mm-view.el. In particular, an Emacs user can be instantly compromised by reading a crafted email message (or Usenet news article).
CVE-2017-14491	Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS response.
CVE-2017-14492	Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted IPv6 router advertisement request.
CVE-2017-14493	Stack-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DHCPv6 request.

CVE-2017-14494	dnsmasq before 2.78, when configured as a relay, allows remote attackers to obtain sensitive memory information via vectors involving handling DHCPv6 forwarded requests.
CVE-2017-14495	Memory leak in dnsmasq before 2.78, when the --add-mac, --add-cpe-id or --add-subnet option is specified, allows remote attackers to cause a denial of service (memory consumption) via vectors involving DNS response creation.
CVE-2017-14496	Integer underflow in the add_pseudoheader function in dnsmasq before 2.78 , when the --add-mac, --add-cpe-id or --add-subnet option is specified, allows remote attackers to cause a denial of service via a crafted DNS request.
CVE-2017-2295	Versions of Puppet prior to 4.10.1 will deserialize data off the wire (from the agent to the server, in this case) with a attacker-specified format. This could be used to force YAML deserialization in an unsafe manner, which would lead to remote code execution. This change constrains the format of data on the wire to PSON or safely decoded YAML.
CVE-2017-2619	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2017-2668	Remote crash via crafted LDAP messages
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-2017-3136	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2017-3137	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When thecandidate has been publicized, the details for this candidate will be

	provided.
CVE-2017-3139	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2017-3142	An error in TSIG authentication can permit unauthorized zone transfers. An attacker may be able to circumvent TSIG authentication of AXFR and Notify requests.
CVE-2017-3143	An error in TSIG authentication can permit unauthorized dynamic updates An attacker may be able to forge a valid TSIG or SIG(0) signature for a dynamic update.
CVE-2017-3167	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.
CVE-2017-3169	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
CVE-2017-3231	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111. 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. 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 v3.0 Base Score 4.3 (Confidentiality impacts).
CVE-2017-3238	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. 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 v3.0 Base Score 6.5 (Availability impacts).
CVE-2017-3241	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. 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 v3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts).
CVE-2017-3243	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Charsets). Supported versions that are affected are 5.5.53 and earlier. 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 v3.0 Base Score 4.4 (Availability impacts).
CVE-2017-3244	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. 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 v3.0 Base Score 6.5 (Availability impacts).
CVE-2017-3252	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JAAS). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, 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, JRockit 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 v3.0 Base Score 5.8 (Integrity impacts).
CVE-2017-3253	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. 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, JRockit. 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 v3.0 Base Score 7.5 (Availability impacts).
CVE-2017-3257	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.6.34 and earlier5.7.16 and earlier. 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 v3.0 Base Score 6.5 (Availability impacts).
CVE-2017-3258	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. 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 v3.0 Base Score 6.5 (Availability impacts).

CVE-2017-3261	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111. 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. 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 v3.0 Base Score 4.3 (Confidentiality impacts).
CVE-2017-3265	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. 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 MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 5.6 (Confidentiality and Availability impacts).
CVE-2017-3272	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111. 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 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 v3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts).
CVE-2017-3273	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.6.34 and earlier and 5.7.16 and earlier. 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 v3.0 Base Score 6.5 (Availability impacts).
CVE-2017-3289	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 7u121 and 8u112; Java SE Embedded: 8u111. 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 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 v3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts).
CVE-2017-3308	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low 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 3.0 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-2017-3309	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low 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 3.0 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-2017-3313	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: MyISAM). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes 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 v3.0 Base Score 4.7 (Confidentiality impacts).
CVE-2017-3317	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Logging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL 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 hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.0 (Availability impacts).
CVE-2017-3318	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Error Handling). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. 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 MySQL

	Server accessible data. CVSS v3.0 Base Score 4.0 (Confidentiality impacts).
CVE-2017-3450	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" 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 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-2017-3453	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. 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-2017-3456	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. 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-2017-3461	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. 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-2017-3462	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. 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-2017-3463	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. 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-2017-3464	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. 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 3.0 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-2017-3509	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121. 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: 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 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N).
CVE-2017-3511	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JCE). Supported versions that are affected are Java SE: 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, Java SE Embedded, JRockit executes to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. 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 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-3526	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. 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, JRockit. 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 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).

CVE-2017-3533	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via FTP to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit 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 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2017-3539	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121. 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 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2017-3544	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SMTP to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE

	Embedded, JRockit 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 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2017-3599	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Pluggable Auth). Supported versions that are affected are 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" 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 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). NOTE: the previous information is from the April 2017 CPU. Oracle has not commented on third-party claims that this issue is an integer overflow in sql/auth/sql_authentication.cc which allows remote attackers to cause a denial of service via a crafted authentication packet.
CVE-2017-3633	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Memcached 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 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:H).
CVE-2017-3634	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.6.36 and earlier and 5.7.18 and earlier. 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-2017-3635	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/C). Supported versions that are affected are 6.1.10 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors. Note: The documentation has also been updated for the correct way to use mysql_stmt_close(). Please see: https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-execute.html, https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-fetch.html, https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-close.html, https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-error.html, https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-errno.html, and https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-sqlstate.html. 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-2017-3636	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.56 and earlier and 5.6.36 and earlier. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes 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 as well as unauthorized read access to a subset of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).
CVE-2017-3641	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. 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-2017-3647	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.36 and earlier and 5.7.18 and earlier. 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-2017-3648	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Charsets). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. 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-2017-3649	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.36 and earlier and 5.7.18 and earlier. 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-2017-3651	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. 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 3.0 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-2017-3652	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit

	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 as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N).
CVE-2017-3653	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit 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 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2017-3731	If an SSL/TLS server or client is running on a 32-bit host, and a specific cipher is being used, then a truncated packet can cause that server or client to perform an out-of-bounds read, usually resulting in a crash. For OpenSSL 1.1.0, the crash can be triggered when using CHACHA20/POLY1305; users should upgrade to 1.1.0d. For Openssl 1.0.2, the crash can be triggered when using RC4-MD5; users who have not disabled that algorithm should update to 1.0.2k.
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-2017-5029	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.
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	Bad cast in Blink
CVE-2017-5053	Out of bounds memory access in V8
CVE-2017-5054	Heap buffer overflow in V8
CVE-2017-5055	Use after free in printing
CVE-2017-5056	Use after free in Blink
CVE-2017-5057	Type confusion in PDFium
CVE-2017-5058	Heap use after free in Print Preview
CVE-2017-5059	Type confusion in Blink
CVE-2017-5060	URL spoofing in Omnibox
CVE-2017-5061	URL spoofing in Omnibox
CVE-2017-5062	Use after free in Chrome Apps
CVE-2017-5063	Heap overflow in Skia
CVE-2017-5064	Use after free in Blink
CVE-2017-5065	Incorrect UI in Blink
CVE-2017-5066	Incorrect signature handing in Networking
CVE-2017-5067	URL spoofing in Omnibox
CVE-2017-5068	Race condition in WebRTC
CVE-2017-5069	Cross-origin bypass in Blink
CVE-2017-5070	Type confusion in V8
CVE-2017-5071	Out of bounds read in V8.
CVE-2017-5072	Address spoofing in Omnibox.
CVE-2017-5073	Use after free in print preview
CVE-2017-5074	Use after free in Apps Bluetooth.
CVE-2017-5075	Information leak in CSP reporting
CVE-2017-5076	Address spoofing in Omnibox.
CVE-2017-5077	Heap buffer overflow in Skia
CVE-2017-5078	Possible command injection in mailto handling
CVE-2017-5079	UI spoofing in Blink
CVE-2017-5080	Use after free in credit card autofill
CVE-2017-5081	Extension verification bypass
CVE-2017-5082	Insufficient hardening in credit card editor
CVE-2017-5083	UI spoofing in Blink
CVE-2017-5085	Inappropriate javascript execution on WebUI pages
CVE-2017-5086	Address spoofing in Omnibox
CVE-2017-5087	Sandbox Escape in IndexedDB
CVE-2017-5088	Out of bounds read in V8
CVE-2017-5089	Domain spoofing in Omnibox
CVE-2017-5091	Use after free in IndexedDB.
CVE-2017-5092	Use after free in PPAPI

CVE-2017-5093	UI spoofing in Blink
CVE-2017-5094	Type confusion in extensions
CVE-2017-5095	Out-of-bounds write in PDFium
CVE-2017-5097	Out-of-bounds read in Skia
CVE-2017-5098	Use after free in V8
CVE-2017-5099	Out-of-bounds write in PPAPI
CVE-2017-5100	Use after free in Chrome Apps
CVE-2017-5101	URL spoofing in OmniBox
CVE-2017-5102	Uninitialized use in Skia
CVE-2017-5103	Uninitialized use in Skia
CVE-2017-5104	UI spoofing in browser
CVE-2017-5105	URL spoofing in OmniBox
CVE-2017-5106	URL spoofing in OmniBox
CVE-2017-5107	User information leak via SVG
CVE-2017-5108	Type confusion in PDFium
CVE-2017-5109	UI spoofing in browser
CVE-2017-5110	UI spoofing in payments dialog
CVE-2017-5111	Use after free in PDFium
CVE-2017-5112	Heap buffer overflow in WebGL
CVE-2017-5113	Heap buffer overflow in Skia
CVE-2017-5114	Memory lifecycle issue in PDFium
CVE-2017-5115	Type confusion in V8
CVE-2017-5116	Type confusion in V8
CVE-2017-5117	Use of uninitialized value in Skia
CVE-2017-5118	Bypass of Content Security Policy in Blink
CVE-2017-5119	Use of uninitialized value in Skia
CVE-2017-5120	Potential HTTPS downgrade during redirect navigation
CVE-2017-5121	Out-of-bounds access in V8
CVE-2017-5122	Out-of-bounds access in V8
CVE-2017-5335	The stream reading functions in lib/opencdk/read-packet.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to cause a denial of service (out-of-memory error and crash) via a crafted OpenPGP certificate.
CVE-2017-5336	Stack-based buffer overflow in the cdk_pk_get_keyid function in lib/opencdk/pubkey.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via a crafted OpenPGP certificate.
CVE-2017-5337	Multiple heap-based buffer overflows in the read_attribute function in GnuTLS before 3.3.26 and

	3.5.x before 3.5.8 allow remote attackers to have unspecified impact via a crafted OpenPGP certificate.
CVE-2017-5340	Zend/zend_hash.c in PHP before 7.0.15 and 7.1.x before 7.1.1 mishandles certain cases that require large array allocations, which allows remote attackers to execute arbitrary code or cause a denial of service (integer overflow, uninitialized memory access, and use of arbitrary destructor function pointers) via crafted serialized data.
CVE-2017-5461	Mozilla Network Security Services (NSS) before 3.21.4, 3.22.x through 3.28.x before 3.28.4, 3.29.x before 3.29.5, and 3.30.x before 3.30.1 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by leveraging incorrect base64 operations.
CVE-2017-5551	The simple_set_acl function in fs/posix_acl.c in the Linux kernel before 4.9.6 preserves the setgid bit during a setxattr call involving a tmpfs filesystem, which allows local users to gain group privileges by leveraging the existence of a setgid program with restrictions on execute permissions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-7097.
CVE-2017-5581	Buffer overflow in the ModifiablePixelBuffer::fillRect function in TigerVNC before 1.7.1 allows remote servers to execute arbitrary code via an RRE message with subrectangle outside framebuffer boundaries.
CVE-2017-5647	A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.
CVE-2017-5648	While investigating bug 60718, it was noticed that some calls to application listeners in Apache Tomcat 9.0.0.M1 to 9.0.0.M17, 8.5.0 to 8.5.11, 8.0.0.RC1 to 8.0.41, and 7.0.0 to 7.0.75 did not use the appropriate facade object. When running an untrusted application under a SecurityManager, it was therefore possible for that untrusted application to retain a reference to the request or response object and thereby access and/or modify information associated with another web application.
CVE-2017-5664	The error page mechanism of the Java Servlet Specification requires that, when an error occurs and an error page is configured for the error that occurred, the original request and response are forwarded to the

	error page. This means that the request is presented to the error page with the original HTTP method. If the error page is a static file, expected behaviour is to serve content of the file as if processing a GET request, regardless of the actual HTTP method. The Default Servlet in Apache Tomcat 9.0.0.M1 to 9.0.0.M20, 8.5.0 to 8.5.14, 8.0.0.RC1 to 8.0.43 and 7.0.0 to 7.0.77 did not do this. Depending on the original request this could lead to unexpected and undesirable results for static error pages including, if the DefaultServlet is configured to permit writes, the replacement or removal of the custom error page. Notes for other user provided error pages: (1) Unless explicitly coded otherwise, JSPs ignore the HTTP method. JSPs used as error pages must must ensure that they handle any error dispatch as a GET request, regardless of the actual method. (2) By default, the response generated by a Servlet does depend on the HTTP method. Custom Servlets used as error pages must ensure that they handle any error dispatch as a GET request, regardless of the actual method.
CVE-2017-5669	The do_shmat function in ipc/shm.c in the Linux kernel through 4.9.12 does not restrict the address calculated by a certain rounding operation, which allows local users to map page zero, and consequently bypass a protection mechanism that exists for the mmap system call, by making crafted shmget and shmat system calls in a privileged context.
CVE-2017-5897	The ip6gre_err function in net/ipv6/ip6_gre.c in the Linux kernel allows remote attackers to have unspecified impact via vectors involving GRE flags in an IPv6 packet, which trigger an out-of-bounds access.
CVE-2017-5953	vim before patch 8.0.0322 does not properly validate values for tree length when handling a spell file, which may result in an integer overflow at a memory allocation site and a resultant buffer overflow.
CVE-2017-5970	The ipv4_pktinfo_prepare function in net/ipv4/ip_sockglue.c in the Linux kernel through 4.9.9 allows attackers to cause a denial of service (system crash) via (1) an application that makes crafted system calls or possibly (2) IPv4 traffic with invalid IP options.
CVE-2017-5986	Race condition in the sctp_wait_for_sndbuf function in net/sctp/socket.c in the Linux kernel before 4.9.11 allows local users to cause a denial of service (assertion failure and panic) via a multithreaded application that peels off an association in a certain buffer-full state.
CVE-2017-6074	The dccp_rcv_state_process function in net/dccp/input.c in the Linux kernel through 4.9.11 mishandles DCCP_PKT_REQUEST packet data structures in the LISTEN state, which allows local users to obtain root

	privileges or cause a denial of service (double free) via an application that makes an IPV6_RECVPKTINFO setsockopt system call.
CVE-2017-6188	Munin before 2.999.6 has a local file write vulnerability when CGI graphs are enabled. Setting multiple upper_limit GET parameters allows overwriting any file accessible to the www-data user.
CVE-2017-6214	The tcp_splice_read function in net/ipv4/tcp.c in the Linux kernel before 4.9.11 allows remote attackers to cause a denial of service (infinite loop and soft lockup) via vectors involving a TCP packet with the URG flag.
CVE-2017-6335	The QuantumTransferMode function in coders/tiff.c in GraphicsMagick 1.3.25 and earlier allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a small samples per pixel value in a CMYKA TIFF file.
CVE-2017-6347	The ip_cmsg_recv_checksum function in net/ipv4/ip_sockglue.c in the Linux kernel before 4.10.1 has incorrect expectations about skb data layout, which allows local users to cause a denial of service (buffer over-read) or possibly have unspecified other impact via crafted system calls, as demonstrated by use of the MSG_MORE flag in conjunction with loopback UDP transmission.
CVE-2017-6349	An integer overflow at a u_read_undo memory allocation site would occur for vim before patch 8.0.0377, if it does not properly validate values for tree length when reading a corrupted undo file, which may lead to resultant buffer overflows.
CVE-2017-6350	An integer overflow at an unserialize_uep memory allocation site would occur for vim before patch 8.0.0378, if it does not properly validate values for tree length when reading a corrupted undo file, which may lead to resultant buffer overflows.
CVE-2017-6353	net/sctp/socket.c in the Linux kernel through 4.10.1 does not properly restrict association peel-off operations during certain wait states, which allows local users to cause a denial of service (invalid unlock and double free) via a multithreaded application. NOTE: this vulnerability exists because of an incorrect fix for CVE-2017-5986.
CVE-2017-6508	CRLF injection vulnerability in the url_parse function in url.c in Wget through 1.19.1 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in the host subcomponent of a URL.
CVE-2017-7000	Pointer disclosure in SQLite
CVE-2017-7184	The xfrm_replay_verify_len function in net/xfrm/xfrm_user.c in the Linux kernel through 4.10.6 does not validate certain size data after an

	XFRM_MSG_NEWAE update, which allows local users to obtain root privileges or cause a denial of service (heap-based out-of-bounds access) by leveraging the CAP_NET_ADMIN capability, as demonstrated during a Pwn2Own competition at CanSecWest 2017 for the Ubuntu 16.10 linux-image-* package 4.8.0.41.52.
CVE-2017-7392	In TigerVNC 1.7.1 (SSecurityVeNCrypt.cxx SSecurityVeNCrypt::SSecurityVeNCrypt), an unauthenticated client can cause a small memory leak in the server.
CVE-2017-7393	In TigerVNC 1.7.1 (VNCSConnectionST.cxx VNCSConnectionST::fence), an authenticated client can cause a double free, leading to denial of service or potentially code execution.
CVE-2017-7394	In TigerVNC 1.7.1 (SSecurityPlain.cxx SSecurityPlain::processMsg), unauthenticated users can crash the server by sending long usernames.
CVE-2017-7395	In TigerVNC 1.7.1 (SMsgReader.cxx SMsgReader::readClientCutText), by causing an integer overflow, an authenticated client can crash the server.
CVE-2017-7396	In TigerVNC 1.7.1 (CConnection.cxx CConnection::CConnection), an unauthenticated client can cause a small memory leak in the server.
CVE-2017-7401	Incorrect interaction of the parse_packet() and parse_part_sign_sha256() functions in network.c in collectd 5.7.1 and earlier allows remote attackers to cause a denial of service (infinite loop) of a collectd instance (configured with "SecurityLevel None" and with empty "AuthFile" options) via a crafted UDP packet.
CVE-2017-7484	It was found that some selectivity estimation functions in PostgreSQL before 9.2.21, 9.3.x before 9.3.17, 9.4.x before 9.4.12, 9.5.x before 9.5.7, and 9.6.x before 9.6.3 did not check user privileges before providing information from pg_statistic, possibly leaking information. An unprivileged attacker could use this flaw to steal some information from tables they are otherwise not allowed to access.
CVE-2017-7485	In PostgreSQL 9.3.x before 9.3.17, 9.4.x before 9.4.12, 9.5.x before 9.5.7, and 9.6.x before 9.6.3, it was found that the PGREQUIRESSL environment variable was no longer enforcing a SSL/TLS connection to a PostgreSQL server. An active Man-in-the-Middle attacker could use this flaw to strip the SSL/TLS protection from a connection between a client and a server.
CVE-2017-7486	PostgreSQL versions 8.4 - 9.6 are vulnerable to information leak in pg_user_mappings view which discloses foreign server passwords to any user having USAGE privilege on the associated foreign server.

CVE-2017-7494	Samba since version 3.5.0 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.
CVE-2017-7502	Null pointer dereference vulnerability in NSS since 3.24.0 was found when server receives empty SSLv2 messages resulting into denial of service by remote attacker.
CVE-2017-7508	OpenVPN versions before 2.4.3 and before 2.3.17 are vulnerable to remote denial-of-service when receiving malformed IPv6 packet.
CVE-2017-7520	OpenVPN versions before 2.4.3 and before 2.3.17 are vulnerable to denial-of-service and/or possibly sensitive memory leak triggered by man-in-the-middle attacker.
CVE-2017-7521	OpenVPN versions before 2.4.3 and before 2.3.17 are vulnerable to remote denial-of-service due to memory exhaustion caused by memory leaks and double-free issue in extract_x509_extension().
CVE-2017-7522	OpenVPN versions before 2.4.3 and before 2.3.17 are vulnerable to denial-of-service by authenticated remote attacker via sending a certificate with an embedded NULL character.
CVE-2017-7529	Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.
CVE-2017-7546	PostgreSQL versions before 9.2.22, 9.3.18, 9.4.13, 9.5.8 and 9.6.4 are vulnerable to incorrect authentication flaw allowing remote attackers to gain access to database accounts with an empty password.
CVE-2017-7547	PostgreSQL versions before 9.2.22, 9.3.18, 9.4.13, 9.5.8 and 9.6.4 are vulnerable to authorization flaw allowing remote authenticated attackers to retrieve passwords from the user mappings defined by the foreign server owners without actually having the privileges to do so.
CVE-2017-7548	PostgreSQL versions before 9.4.13, 9.5.8 and 9.6.4 are vulnerable to authorization flaw allowing remote authenticated attackers with no privileges on a large object to overwrite the entire contents of the object, resulting in a denial of service.
CVE-2017-7551	389-ds-base version before 1.3.5.19 and 1.3.6.7 are vulnerable to password brute-force attacks during account lockout due to different return codes returned on password attempts.
CVE-2017-7659	A maliciously constructed HTTP/2 request could cause mod_http2 2.4.24, 2.4.25 to dereference a NULL pointer and crash the server process.

CVE-2017-7668	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.
CVE-2017-7674	The CORS Filter in Apache Tomcat 9.0.0.M1 to 9.0.0.M21, 8.5.0 to 8.5.15, 8.0.0.RC1 to 8.0.44 and 7.0.41 to 7.0.78 did not add an HTTP Vary header indicating that the response varies depending on Origin. This permitted client and server side cache poisoning in some circumstances.
CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2017-7771	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2017-7772	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2017-7773	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2017-7774	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When thecandidate has been publicized, the details for this candidate will be provided.
CVE-2017-7775	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2017-7776	** RESERVED **

	This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2017-7777	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2017-7778	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2017-7805	Use-after-free in TLS 1.2 generating handshake hashes
CVE-2017-7890	The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.31 and 7.x before 7.1.7, does not zero colorMap arrays before use. A specially crafted GIF image could use the uninitialized tables to read ~700 bytes from the top of the stack, potentially disclosing sensitive information.
CVE-2017-8108	Unspecified tests in Lynis before 2.5.0 allow local users to write to arbitrary files or possibly gain privileges via a symlink attack on a temporary file.
CVE-2017-8291	Artifex Ghostscript through 2017-04-26 allows -dSAFER bypass and remote command execution via .rsdparams type confusion with a "/OutputFile (%pipe%" substring in a crafted .eps document that is an input to the gs program, as exploited in the wild in April 2017.
CVE-2017-8386	git-shell in git before 2.4.12, 2.5.x before 2.5.6, 2.6.x before 2.6.7, 2.7.x before 2.7.5, 2.8.x before 2.8.5, 2.9.x before 2.9.4, 2.10.x before 2.10.3, 2.11.x before 2.11.2, and 2.12.x before 2.12.3 might allow remote authenticated users to gain privileges via a repository name that starts with a - (dash) character.
CVE-2017-8714	The Windows Hyper-V component on Microsoft Windows 8.1, Windows Server 2012 Gold and R2,, Windows 10 1607, and Windows Server 2016 allows a remote code execution vulnerability when it fails to properly validate input from an authenticated user on a guest operating system, aka "Remote Desktop Virtual Host Remote Code Execution Vulnerability".
CVE-2017-8779	rpcbind through 0.2.4, LIBTIRPC through 1.0.1 and 1.0.2-rc through 1.0.2-rc3, and NTIRPC through 1.4.3 do not consider the maximum RPC data size during memory allocation for XDR strings, which allows

	remote attackers to cause a denial of service (memory consumption with no subsequent free) via a crafted UDP packet to port 111, aka rpcbomb.
CVE-2017-8932	A bug in the standard library ScalarMult implementation of curve P-256 for amd64 architectures in Go before 1.7.6 and 1.8.x before 1.8.2 causes incorrect results to be generated for specific input points. An adaptive attack can be mounted to progressively extract the scalar input to ScalarMult by submitting crafted points and observing failures to the derive correct output. This leads to a full key recovery attack against static ECDH, as used in popular JWT libraries.
CVE-2017-9224	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds read occurs in match_at() during regular expression searching. A logical error involving order of validation and access in match_at() could result in an out-of-bounds read from a stack buffer.
CVE-2017-9226	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A heap out-of-bounds write or read occurs in next_state_val() during regular expression compilation. Octal numbers larger than 0xff are not handled correctly in fetch_token() and fetch_token_in_cc(). A malformed regular expression containing an octal number in the form of '\700' would produce an invalid code point value larger than 0xff in next_state_val(), resulting in an out-of-bounds write memory corruption.
CVE-2017-9227	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds read occurs in mbc_enc_len() during regular expression searching. Invalid handling of reg->dmin in forward_search_range() could result in an invalid pointer dereference, as an out-of-bounds read from a stack buffer.
CVE-2017-9228	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A heap out-of-bounds write occurs in bitset_set_range() during regular expression compilation due to an uninitialized variable from an incorrect state transition. An incorrect state transition in parse_char_class() could create an execution path that leaves a critical local variable uninitialized until it's used as an index, resulting in an out-of-bounds write memory corruption.
CVE-2017-9229	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A SIGSEGV

	occurs in left_adjust_char_head() during regular expression compilation. Invalid handling of reg->dmax in forward_search_range() could result in an invalid pointer dereference, normally as an immediate denial-of-service condition.
CVE-2017-9450	** RESERVED ** This candidate has been reserved by an organization or individual thatwill use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will beprovided.
CVE-2017-9462	In Mercurial before 4.1.3, "hg serve --stdio" allows remote authenticated users to launch the Python debugger, and consequently execute arbitrary code, by using --debugger as a repository name.
CVE-2017-9775	Stack buffer overflow in GfxState.cc in pdftocairo in Poppler before 0.56 allows remote attackers to cause a denial of service (application crash) via a crafted PDF document.
CVE-2017-9776	Integer overflow leading to Heap buffer overflow in JBIG2Stream.cc in pdftocairo in Poppler before 0.56 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PDF document.
CVE-2017-9788	In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.
CVE-2017-9798	Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.
CVE-2017-9800	A maliciously constructed svn+ssh:// URL would cause Subversion clients before 1.8.19, 1.9.x before 1.9.7, and 1.10.0.x through 1.10.0-alpha3 to run an arbitrary shell command. Such a URL could be generated by a malicious server, by a malicious user committing to a honest server (to attack another user of that server's

	repositories), or by a proxy server. The vulnerability affects all clients, including those that use file://, http://, and plain (untunneled) svn://.