Amazon Inspector - Assessment Report

Full Report

Report generated on 2018-12-10 at 13:36:28 UTC

Assessment Template: Lab7Assessment

Assessment Run start: 2018-12-10 at 12:35:46 UTC
Assessment Run end: 2018-12-10 at 12:52:07 UTC

Section 1: Executive Summary

This is an Inspector assessment report for an assessment started on 2018-12-10 12:35:46 UTC for assessment template 'Lab7Assessment'. The assessment target included 1 instances, and was tested against 2 Rules Packages.

The assessment target is defined using the following EC2 tags

Key	Value
Name	Lab7-Jump

The following Rules Packages were assessed. A total of 33 findings were created, with the following distribution by severity:

Rules Package	High	Medium	Low	Informational
Common Vulnerabilities and Exposures-1.1	17	13	2	0
Security Best Practices-1.0	0	1	0	0

Section 2: What is Tested

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

2.1: Rules Packages - Count: 2

2.1.1: Common Vulnerabilities and Exposures-1.1

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

2.1.2: Security Best Practices-1.0

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

2.2: Assessment Target - Lab7Assessment

2.2.1: EC2 Tags:

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

Key	Value
Name	Lab7-Jump

2.2.2: Instances - Count 1

Instance ID
i-010f52774617e4247

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-2017-13168	Medium	1
CVE-2018-0734	Medium	1
CVE-2018-0735	Medium	1
CVE-2018-10853	Medium	1
CVE-2018-14618	High	1
CVE-2018-14633	High	1
CVE-2018-15471	High	1
CVE-2018-15473	High	1
CVE-2018-15572	Medium	1
CVE-2018-15594	Medium	1
CVE-2018-15686	Low	1
CVE-2018-15687	Medium	1
CVE-2018-15688	High	1
CVE-2018-16428	High	1
CVE-2018-16429	High	1
CVE-2018-16658	Medium	1
CVE-2018-16839	High	1
CVE-2018-16840	High	1
CVE-2018-16842	High	1
CVE-2018-17182	High	1
CVE-2018-17456	High	1
CVE-2018-18074	High	1
CVE-2018-18584	Medium	1
CVE-2018-18585	Low	1

CVE-2018-18955	High	1
CVE-2018-19486	High	1
CVE-2018-5407	Medium	1
CVE-2018-6554	Medium	1
CVE-2018-6555	High	1
CVE-2018-6559	Medium	1
CVE-2018-6954	High	1
CVE-2018-9363	Medium	1

3.2: Findings table - Security Best Practices-1.0

Rule	Severity	Failed
Disable root login over SSH	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-2017-13168

Severity
Medium

Description
An elevation of privilege vulnerability in the kernel scsi driver. Product: Android. Versions: Android kernel. Android ID A-65023233.

Recommendation
Use your Operating System's update feature to update package linux-image-4.15.0-1021-aws-0:4.15.0-1021.21, linux-image-aws-0:4.15.0.1021.21-0. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-13168

Failed Instances
i-010f52774617e4247

CVE-2018-0734

Severity
Medium

Description
The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).

Recommendation
Use your Operating System's update feature to update package libssl1.0.0-0:1.0.2n-1ubuntu5.1, libssl1.1-0:1.1.0g-2ubuntu4.1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0734

Failed Instances
i-010f52774617e4247

CVE-2018-0735

Severity
Medium

Description
The OpenSSL ECDSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.1.1a (Affected 1.1.1).

Recommendation
Use your Operating System's update feature to update package libssl1.0.0-0:1.0.2n-1ubuntu5.1, libssl1.1-0:1.1.0g-2ubuntu4.1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-0735

Failed Instances
i-010f52774617e4247

CVE-2018-10853

Severity
Medium

Description
A flaw was found in the way Linux kernel KVM hypervisor before 4.18 emulated instructions such as sgdt/sidt/fxsave/fxrstor. It did not check current privilege(CPL) level while emulating unprivileged instructions. An unprivileged guest user/process could use this flaw to potentially escalate privileges inside guest.

Recommendation

Use your Operating System's update feature to update package linux-image-4.15.0-1021-aws-0:4.15.0-1021.21, linux-image-aws-0:4.15.0.1021.21-0. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10853

Failed Instances
i-010f52774617e4247

CVE-2018-14618

Severity
High

Description
curl before version 7.61.1 is vulnerable to a buffer overrun in the NTLM authentication code. The internal function Curl_ntlm_core_mk_nt_hash multiplies the length of the password by two (SUM) to figure out how large temporary storage area to allocate from the heap. The length value is then subsequently used to iterate over the password and generate output into the allocated storage buffer. On systems with a 32 bit size_t, the math to calculate SUM triggers an integer overflow when the password length exceeds 2GB (2^31 bytes). This integer overflow usually causes a very small buffer to actually get allocated instead of the intended very huge one, making the use of that buffer end up in a heap buffer overflow. (This bug is almost identical to CVE-2017-8816.)

Recommendation
Use your Operating System's update feature to update package curl-0:7.58.0-2ubuntu3.2, libcurl3-gnutls-0:7.58.0-2ubuntu3.2, libcurl4-0:7.58.0-2ubuntu3.2. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14618

Failed Instances
i-010f52774617e4247

CVE-2018-14633

Severity
High

Description
A security flaw was found in the chap_server_compute_md5() function in the ISCSI target code in the Linux kernel in a way an authentication request from an ISCSI

initiator is processed. An unauthenticated remote attacker can cause a stack buffer overflow and smash up to 17 bytes of the stack. The attack requires the iSCSI target to be enabled on the victim host. Depending on how the target's code was built (i.e. depending on a compiler, compile flags and hardware architecture) an attack may lead to a system crash and thus to a denial-of-service or possibly to a non-authorized access to data exported by an iSCSI target. Due to the nature of the flaw, privilege escalation cannot be fully ruled out, although we believe it is highly unlikely. Kernel versions 4.18.x, 4.14.x and 3.10.x are believed to be vulnerable.

Recommendation
Use your Operating System's update feature to update package linux-image-4.15.0-1021-aws-0:4.15.0-1021.21, linux-image-aws-0:4.15.0.1021.21-0. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14633

Failed Instances
i-010f52774617e4247

CVE-2018-15471

Severity
High

Description
An issue was discovered in xenvif_set_hash_mapping in drivers/net/xen-netback/hash.c in the Linux kernel through 4.18.1, as used in Xen through 4.11.x and other products. The Linux netback driver allows frontends to control mapping of requests to request queues. When processing a request to set or change this mapping, some input validation (e.g., for an integer overflow) was missing or flawed, leading to OOB access in hash handling. A malicious or buggy frontend may cause the (usually privileged) backend to make out of bounds memory accesses, potentially resulting in one or more of privilege escalation, Denial of Service (DoS), or information leaks.

Recommendation
Use your Operating System's update feature to update package linux-image-4.15.0-1021-aws-0:4.15.0-1021.21, linux-image-aws-0:4.15.0.1021.21-0. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15471

Failed Instances
i-010f52774617e4247

CVE-2018-15473

Severity
High

Description
OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.

Recommendation
Use your Operating System's update feature to update package openssh-server-1:7.6p1-4. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15473

Failed Instances
i-010f52774617e4247

CVE-2018-15572

Severity
Medium

Description
The spectre_v2_select_mitigation function in arch/x86/kernel/cpu/bugs.c in the Linux kernel before 4.18.1 does not always fill RSB upon a context switch, which makes it easier for attackers to conduct userspace-userspace spectreRSB attacks.

Recommendation
Use your Operating System's update feature to update package linux-image-4.15.0-1021-aws-0:4.15.0-1021.21, linux-image-aws-0:4.15.0.1021.21-0. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15572

Failed Instances
i-010f52774617e4247

CVE-2018-15594

Severity
Medium

Description
arch/x86/kernel/paravirt.c in the Linux kernel before 4.18.1 mishandles certain indirect calls, which makes it easier for attackers to conduct Spectre-v2 attacks against paravirtual guests.

Recommendation
Use your Operating System's update feature to update package linux-image-4.15.0-1021-aws-0:4.15.0-1021.21, linux-image-aws-0:4.15.0.1021.21-0. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15594

Failed Instances
i-010f52774617e4247

CVE-2018-15686

Severity
Low

Description
A vulnerability in unit_deserialize of systemd allows an attacker to supply arbitrary state across systemd re-execution via NotifyAccess. This can be used to improperly influence systemd execution and possibly lead to root privilege escalation. Affected releases are systemd versions up to and including 239.

Recommendation
Use your Operating System's update feature to update package systemd-0:237-3ubuntu10.3. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15686

Failed Instances
i-010f52774617e4247

CVE-2018-15687

Severity
Medium

Description

A race condition in chown_one() of systemd allows an attacker to cause systemd to set arbitrary permissions on arbitrary files. Affected releases are systemd versions up to and including 239.

Recommendation
Use your Operating System's update feature to update package systemd-0:237-3ubuntu10.3. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15687

Failed Instances
i-010f52774617e4247

CVE-2018-15688

Severity
High

Description
A buffer overflow vulnerability in the dhcp6 client of systemd allows a malicious dhcp6 server to overwrite heap memory in systemd-networkd. Affected releases are systemd: versions up to and including 239.

Recommendation
Use your Operating System's update feature to update package systemd-0:237-3ubuntu10.3. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-15688

Failed Instances
i-010f52774617e4247

CVE-2018-16428

Severity
High

Description
In GNOME GLib 2.56.1, g_markup_parse_context_end_parse() in gmarkup.c has a NULL pointer dereference.

Recommendation

Use your Operating System's update feature to update package libglib2.0-0-0:2.56.2-0ubuntu0.18.04.1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16428

Failed Instances
i-010f52774617e4247

CVE-2018-16429

Severity
High

Description
GNOME GLib 2.56.1 has an out-of-bounds read vulnerability in g_markup_parse_context_parse() in gmarkup.c, related to utf8_str().

Recommendation
Use your Operating System's update feature to update package libglib2.0-0-0:2.56.2-0ubuntu0.18.04.1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16429

Failed Instances
i-010f52774617e4247

CVE-2018-16658

Severity
Medium

Description
An issue was discovered in the Linux kernel before 4.18.6. An information leak in cdrom_ioctl_drive_status in drivers/cdrom/cdrom.c could be used by local attackers to read kernel memory because a cast from unsigned long to int interferes with bounds checking. This is similar to CVE-2018-10940.

Recommendation
Use your Operating System's update feature to update package linux-image-4.15.0-1021-aws-0:4.15.0-1021.21, linux-image-aws-0:4.15.0.1021.21-0. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16658

Failed Instances

i-010f52774617e4247

CVE-2018-16839

Severity
High

Description
Curl versions 7.33.0 through 7.61.1 are vulnerable to a buffer overrun in the SASL authentication code that may lead to denial of service.

Recommendation
Use your Operating System's update feature to update package curl-0:7.58.0-2ubuntu3.2, libcurl3-gnutls-0:7.58.0-2ubuntu3.2, libcurl4-0:7.58.0-2ubuntu3.2. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16839

Failed Instances
i-010f52774617e4247

CVE-2018-16840

Severity
High

Description
A heap use-after-free flaw was found in curl versions from 7.59.0 through 7.61.1 in the code related to closing an easy handle. When closing and cleaning up an 'easy' handle in the `Curl_close()` function, the library code first frees a struct (without nulling the pointer) and might then subsequently erroneously write to a struct field within that already freed struct.

Recommendation
Use your Operating System's update feature to update package curl-0:7.58.0-2ubuntu3.2, libcurl3-gnutls-0:7.58.0-2ubuntu3.2, libcurl4-0:7.58.0-2ubuntu3.2. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16840

Failed Instances
i-010f52774617e4247

CVE-2018-16842

Severity
High

Description
Curl versions 7.14.1 through 7.61.1 are vulnerable to a heap-based buffer over-read in the tool_msgs.c:voutf() function that may result in information exposure and denial of service.

Recommendation
Use your Operating System's update feature to update package curl-0:7.58.0-2ubuntu3.2, libcurl3-gnutls-0:7.58.0-2ubuntu3.2, libcurl4-0:7.58.0-2ubuntu3.2. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16842

Failed Instances
i-010f52774617e4247

CVE-2018-17182

Severity
High

Description
An issue was discovered in the Linux kernel through 4.18.8. The vmacache_flush_all function in mm/vmacache.c mishandles sequence number overflows. An attacker can trigger a use-after-free (and possibly gain privileges) via certain thread creation, map, unmap, invalidation, and dereference operations.

Recommendation
Use your Operating System's update feature to update package linux-image-4.15.0-1021-aws-0:4.15.0-1021.21, linux-image-aws-0:4.15.0.1021.21-0. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17182

Failed Instances
i-010f52774617e4247

CVE-2018-17456

Severity
High

Description
Git before 2.14.5, 2.15.x before 2.15.3, 2.16.x before 2.16.5, 2.17.x before 2.17.2, 2.18.x before 2.18.1, and 2.19.x before 2.19.1 allows remote code execution during processing of a recursive "git clone" of a superproject if a .gitmodules file has a URL field beginning with a '-' character.

Recommendation
Use your Operating System's update feature to update package git-1:2.17.1-1ubuntu0.1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17456

Failed Instances
i-010f52774617e4247

CVE-2018-18074

Severity
High

Description
The Requests package before 2.20.0 for Python sends an HTTP Authorization header to an http URI upon receiving a same-hostname https-to-http redirect, which makes it easier for remote attackers to discover credentials by sniffing the network.

Recommendation
Use your Operating System's update feature to update package python3-requests-0:2.18.4-2. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18074

Failed Instances
i-010f52774617e4247

CVE-2018-18584

Severity
Medium

Description

In mspack/cab.h in libmspack before 0.8alpha and cabextract before 1.8, the CAB block input buffer is one byte too small for the maximal Quantum block, leading to an out-of-bounds write.

Recommendation
Use your Operating System's update feature to update package libmspack0-0:0.6-3ubuntu0.1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18584

Failed Instances
i-010f52774617e4247

CVE-2018-18585

Severity
Low

Description
chmd_read_headers in mspack/chmd.c in libmspack before 0.8alpha accepts a filename that has '\0' as its first or second character (such as the "/\0" name).

Recommendation
Use your Operating System's update feature to update package libmspack0-0:0.6-3ubuntu0.1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18585

Failed Instances
i-010f52774617e4247

CVE-2018-18955

Severity
High

Description
In the Linux kernel 4.15.x through 4.19.x before 4.19.2, map_write() in kernel/user_namespace.c allows privilege escalation because it mishandles nested user namespaces with more than 5 UID or GID ranges. A user who has CAP_SYS_ADMIN in an affected user namespace can bypass access controls on resources outside the namespace, as demonstrated by reading /etc/shadow. This occurs because an ID

transformation takes place properly for the namespaced-to-kernel direction but not for the kernel-to-namespaced direction.

Recommendation
Use your Operating System's update feature to update package linux-image-4.15.0-1021-aws-0:4.15.0-1021.21, linux-image-aws-0:4.15.0.1021.21-0. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18955

Failed Instances
i-010f52774617e4247

CVE-2018-19486

Severity
High

Description
Git before 2.19.2 on Linux and UNIX executes commands from the current working directory (as if '.' were at the end of $PATH) in certain cases involving the run_command() API and run-command.c, because there was a dangerous change from execvp to execv during 2017.

Recommendation
Use your Operating System's update feature to update package git-1:2.17.1-1ubuntu0.1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19486

Failed Instances
i-010f52774617e4247

CVE-2018-5407

Severity
Medium

Description
Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.

Recommendation

Use your Operating System's update feature to update package libssl1.0.0-0:1.0.2n-1ubuntu5.1, libssl1.1-0:1.1.0g-2ubuntu4.1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-5407

Failed Instances
i-010f52774617e4247

CVE-2018-6554

Severity
Medium

Description
Memory leak in the irda_bind function in net/irda/af_irda.c and later in drivers/staging/irda/net/af_irda.c in the Linux kernel before 4.17 allows local users to cause a denial of service (memory consumption) by repeatedly binding an AF_IRDA socket.

Recommendation
Use your Operating System's update feature to update package linux-image-4.15.0-1021-aws-0:4.15.0-1021.21, linux-image-aws-0:4.15.0.1021.21-0. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6554

Failed Instances
i-010f52774617e4247

CVE-2018-6555

Severity
High

Description
The irda_setsockopt function in net/irda/af_irda.c and later in drivers/staging/irda/net/af_irda.c in the Linux kernel before 4.17 allows local users to cause a denial of service (ias_object use-after-free and system crash) or possibly have unspecified other impact via an AF_IRDA socket.

Recommendation
Use your Operating System's update feature to update package linux-image-4.15.0-1021-aws-0:4.15.0-1021.21, linux-image-aws-0:4.15.0.1021.21-0. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6555

Failed Instances
i-010f52774617e4247

CVE-2018-6559

Severity
Medium

Description
The Linux kernel, as used in Ubuntu 18.04 LTS and Ubuntu 18.10, allows local users to obtain names of files in which they would not normally be able to access via an overlayfs mount inside of a user namespace.

Recommendation
Use your Operating System's update feature to update package linux-image-4.15.0-1021-aws-0:4.15.0-1021.21, linux-image-aws-0:4.15.0.1021.21-0. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6559

Failed Instances
i-010f52774617e4247

CVE-2018-6954

Severity
High

Description
systemd-tmpfiles in systemd through 237 mishandles symlinks present in non-terminal path components, which allows local users to obtain ownership of arbitrary files via vectors involving creation of a directory and a file under that directory, and later replacing that directory with a symlink. This occurs even if the fs.protected_symlinks sysctl is turned on.

Recommendation
Use your Operating System's update feature to update package systemd-0:237-3ubuntu10.3. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-6954

Failed Instances
i-010f52774617e4247

CVE-2018-9363

Severity
Medium

Description
In the hidp_process_report in bluetooth, there is an integer overflow. This could lead to an out of bounds write with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-65853588 References: Upstream kernel.

Recommendation
Use your Operating System's update feature to update package linux-image-4.15.0-1021-aws-0:4.15.0-1021.21, linux-image-aws-0:4.15.0.1021.21-0. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-9363

Failed Instances
i-010f52774617e4247

4.2: Findings details - Security Best Practices-1.0

Disable root login over SSH

Severity
Medium

Description
This rule helps determine whether the SSH daemon is configured to permit logging in to your EC2 instance as root.

Recommendation
To reduce the likelihood of a successful brute-force attack, we recommend that you configure your EC2 instance to prevent root account logins over SSH. To disable SSH root account logins, set PermitRootLogin to 'no' in /etc/ssh/sshd_config and restart sshd. When logged in as a non-root user, you can use sudo to escalate privileges when necessary. If you want to allow public key authentication with a command associated with the key, you can set PermitRootLogin to 'forced-commands-only'.

Failed Instances
i-010f52774617e4247

Section 5: Passed Rules

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

5.1 Passed rules - Common Vulnerabilities and Exposures-1.1

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CVE-2013-2735	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2736	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2737	A JavaScript API in Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allows attackers to obtain sensitive information via unspecified vectors.
CVE-2013-2741	importbuddy.php in the BackupBuddy plugin 1.3.4, 2.1.4, 2.2.25, 2.2.28, and 2.2.4 for WordPress does not require that authentication be enabled, which allows remote attackers to obtain sensitive information, or overwrite or delete files, via vectors involving a (1) direct request, (2) step=1 request, (3) step=2 or step=3 request, or (4) step=7 request.
CVE-2013-2766	Cross-site scripting (XSS) vulnerability in Splunk Web in Splunk 4.3.0 through 4.3.5 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2013-2836	Multiple unspecified vulnerabilities in Google Chrome before 27.0.1453.93 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2837	Use-after-free vulnerability in the SVG implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2838	Google V8, as used in Google Chrome before 27.0.1453.93, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2013-2839	Google Chrome before 27.0.1453.93 does not properly perform a cast of an unspecified variable during

	handling of clipboard data, which allows remote attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2840	Use-after-free vulnerability in the media loader in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2013-2846.
CVE-2013-2841	Use-after-free vulnerability in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of Pepper resources.
CVE-2013-2842	Use-after-free vulnerability in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of widgets.
CVE-2013-2843	Use-after-free vulnerability in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of speech data.
CVE-2013-2844	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to style resolution.
CVE-2013-2845	The Web Audio implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2846	Use-after-free vulnerability in the media loader in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2013-2840.
CVE-2013-2847	Race condition in the workers implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2848	The XSS Auditor in Google Chrome before 27.0.1453.93 might allow remote attackers to obtain sensitive information via unspecified vectors.
CVE-2013-2849	Multiple cross-site scripting (XSS) vulnerabilities in Google Chrome before 27.0.1453.93 allow user-assisted remote attackers to inject arbitrary web script or HTML via vectors involving a (1) drag-and-drop or (2) copy-and-paste operation.
CVE-2013-2853	The HTTPS implementation in Google Chrome before 28.0.1500.71 does not ensure that headers are

	terminated by \r\n\r\n (carriage return, newline, carriage return, newline), which allows man-in-the-middle attackers to have an unspecified impact via vectors that trigger header truncation.
CVE-2013-2855	The Developer Tools API in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2856	Use-after-free vulnerability in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of input.
CVE-2013-2857	Use-after-free vulnerability in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of images.
CVE-2013-2858	Use-after-free vulnerability in the HTML5 Audio implementation in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2859	Google Chrome before 27.0.1453.110 allows remote attackers to bypass the Same Origin Policy and trigger namespace pollution via unspecified vectors.
CVE-2013-2860	Use-after-free vulnerability in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving access to a database API by a worker process.
CVE-2013-2861	Use-after-free vulnerability in the SVG implementation in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2862	Skia, as used in Google Chrome before 27.0.1453.110, does not properly handle GPU acceleration, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2863	Google Chrome before 27.0.1453.110 does not properly handle SSL sockets, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-2864	The PDF functionality in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service (invalid free operation) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2865	Multiple unspecified vulnerabilities in Google Chrome before 27.0.1453.110 allow attackers to cause a denial

	of service or possibly have other impact via unknown vectors.
CVE-2013-2867	Google Chrome before 28.0.1500.71 does not properly prevent pop-under windows, which allows remote attackers to have an unspecified impact via a crafted web site.
CVE-2013-2868	common/extensions/sync_helper.cc in Google Chrome before 28.0.1500.71 proceeds with sync operations for NPAPI extensions without checking for a certain plugin permission setting, which might allow remote attackers to trigger unwanted extension changes via unspecified vectors.
CVE-2013-2869	Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted JPEG2000 image.
CVE-2013-2870	Use-after-free vulnerability in Google Chrome before 28.0.1500.71 allows remote servers to execute arbitrary code via crafted response traffic after a URL request.
CVE-2013-2871	Use-after-free vulnerability in Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of input.
CVE-2013-2873	Use-after-free vulnerability in Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a 404 HTTP status code during the loading of resources.
CVE-2013-2875	core/rendering/svg/SVGInlineTextBox.cpp in the SVG implementation in Blink, as used in Google Chrome before 28.0.1500.71, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2013-2876	browser/extensions/api/tabs/tabs_api.cc in Google Chrome before 28.0.1500.71 does not properly enforce restrictions on the capture of screenshots by extensions, which allows remote attackers to obtain sensitive information about the content of a previous page via vectors involving an interstitial page.
CVE-2013-2877	parser.c in libxml2 before 2.9.0, as used in Google Chrome before 28.0.1500.71 and other products, allows remote attackers to cause a denial of service (out-of-bounds read) via a document that ends abruptly, related to the lack of certain checks for the XML_PARSER_EOF state.
CVE-2013-2878	Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the handling of text.
CVE-2013-2879	Google Chrome before 28.0.1500.71 does not properly determine the circumstances in which a renderer

	process can be considered a trusted process for sign-in and subsequent sync operations, which makes it easier for remote attackers to conduct phishing attacks via a crafted web site.
CVE-2013-2880	Multiple unspecified vulnerabilities in Google Chrome before 28.0.1500.71 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2881	Google Chrome before 28.0.1500.95 does not properly handle frames, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2013-2882	Google V8, as used in Google Chrome before 28.0.1500.95, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2013-2883	Use-after-free vulnerability in Google Chrome before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to deleting the registration of a MutationObserver object.
CVE-2013-2884	Use-after-free vulnerability in the DOM implementation in Google Chrome before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to improper tracking of which document owns an Attr object.
CVE-2013-2885	Use-after-free vulnerability in Google Chrome before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to not properly considering focus during the processing of JavaScript events in the presence of a multiple-fields input type.
CVE-2013-2886	Multiple unspecified vulnerabilities in Google Chrome before 28.0.1500.95 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2887	Multiple unspecified vulnerabilities in Google Chrome before 29.0.1547.57 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2900	The FilePath::ReferencesParent function in files/file_path.cc in Google Chrome before 29.0.1547.57 on Windows does not properly handle pathname components composed entirely of . (dot) and whitespace characters, which allows remote attackers to conduct directory traversal attacks via a crafted directory name.
CVE-2013-2901	Multiple integer overflows in (1) libGLESv2/renderer/Renderer9.cpp and (2) libGLESv2/renderer/Renderer11.cpp in Almost Native Graphics Layer

	Engine (ANGLE), as used in Google Chrome before 29.0.1547.57, allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2902	Use-after-free vulnerability in the XSLT ProcessingInstruction implementation in Blink, as used in Google Chrome before 29.0.1547.57, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to an applyXSLTransform call involving (1) an HTML document or (2) an xsl:processing-instruction element that is still in the process of loading.
CVE-2013-2903	Use-after-free vulnerability in the HTMLMediaElement::didMoveToNewDocument function in core/html/HTMLMediaElement.cpp in Blink, as used in Google Chrome before 29.0.1547.57, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving moving a (1) AUDIO or (2) VIDEO element between documents.
CVE-2013-2904	Use-after-free vulnerability in the Document::finishedParsing function in core/dom/Document.cpp in Blink, as used in Google Chrome before 29.0.1547.57, allows remote attackers to cause a denial of service or possibly have unspecified other impact via an onload event that changes an IFRAME element so that its src attribute is no longer an XML document, leading to unintended garbage collection of this document.
CVE-2013-2905	The SharedMemory::Create function in memory/shared_memory_posix.cc in Google Chrome before 29.0.1547.57 uses weak permissions under /dev/shm/, which allows attackers to obtain sensitive information via direct access to a POSIX shared-memory file.
CVE-2013-2906	Multiple race conditions in the Web Audio implementation in Blink, as used in Google Chrome before 30.0.1599.66, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to threading in core/html/HTMLMediaElement.cpp, core/platform/audio/AudioDSPKernelProcessor.cpp, core/platform/audio/HRTFElevation.cpp, and modules/webaudio/ConvolverNode.cpp.
CVE-2013-2907	The Window.prototype object implementation in Google Chrome before 30.0.1599.66 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2013-2908	Google Chrome before 30.0.1599.66 uses incorrect function calls to determine the values of NavigationEntry objects, which allows remote attackers

	to spoof the address bar via vectors involving a response with a 204 (aka No Content) status code.
CVE-2013-2909	Use-after-free vulnerability in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to inline-block rendering for bidirectional Unicode text in an element isolated from its siblings.
CVE-2013-2910	Use-after-free vulnerability in modules/webaudio/AudioScheduledSourceNode.cpp in the Web Audio implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2911	Use-after-free vulnerability in the XSLStyleSheet::compileStyleSheet function in core/xml/XSLStyleSheetLibxslt.cpp in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of post-failure recompilation in unspecified libxslt versions.
CVE-2013-2912	Use-after-free vulnerability in the PepperInProcessRouter::SendToHost function in content/renderer/pepper/pepper_in_process_router.cc in the Pepper Plug-in API (PPAPI) in Google Chrome before 30.0.1599.66 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a resource-destruction message.
CVE-2013-2913	Use-after-free vulnerability in the XMLDocumentParser::append function in core/xml/parser/XMLDocumentParser.cpp in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving an XML document.
CVE-2013-2915	Google Chrome before 30.0.1599.66 preserves pending NavigationEntry objects in certain invalid circumstances, which allows remote attackers to spoof the address bar via a URL with a malformed scheme, as demonstrated by a nonexistent:12121 URL.
CVE-2013-2916	Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to spoof the address bar via vectors involving a response with a 204 (aka No Content) status code, in conjunction with a delay in notifying the user of an attempted spoof.
CVE-2013-2917	The ReverbConvolverStage::ReverbConvolverStage function in core/platform/audio/ReverbConvolverStage.cpp in the Web Audio

	implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the impulseResponse array.
CVE-2013-2918	Use-after-free vulnerability in the RenderBlock::collapseAnonymousBlockChild function in core/rendering/RenderBlock.cpp in the DOM implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect handling of parent-child relationships for anonymous blocks.
CVE-2013-2919	Google V8, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2920	The DoResolveRelativeHost function in url/url_canon_relative.cc in Google Chrome before 30.0.1599.66 allows remote attackers to cause a denial of service (out-of-bounds read) via a relative URL containing a hostname, as demonstrated by a protocol-relative URL beginning with a //www.google.com/ substring.
CVE-2013-2921	Double free vulnerability in the ResourceFetcher::didLoadResource function in core/fetch/ResourceFetcher.cpp in the resource loader in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering certain callback processing during the reporting of a resource entry.
CVE-2013-2922	Use-after-free vulnerability in core/html/HTMLTemplateElement.cpp in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that operates on a TEMPLATE element.
CVE-2013-2923	Multiple unspecified vulnerabilities in Google Chrome before 30.0.1599.66 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2924	Use-after-free vulnerability in International Components for Unicode (ICU), as used in Google Chrome before 30.0.1599.66 and other products, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2925	Use-after-free vulnerability in core/xml/XMLHttpRequest.cpp in Blink, as used in Google Chrome before 30.0.1599.101, allows remote attackers to cause a denial of service or possibly have

	unspecified other impact via vectors that trigger multiple conflicting uses of the same XMLHttpRequest object.
CVE-2013-2926	Use-after-free vulnerability in the IndentOutdentCommand::tryIndentingAsListItem function in core/editing/IndentOutdentCommand.cpp in Blink, as used in Google Chrome before 30.0.1599.101, allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to list elements.
CVE-2013-2927	Use-after-free vulnerability in the HTMLFormElement::prepareForSubmission function in core/html/HTMLFormElement.cpp in Blink, as used in Google Chrome before 30.0.1599.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to submission for FORM elements.
CVE-2013-2928	Multiple unspecified vulnerabilities in Google Chrome before 30.0.1599.101 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2931	Multiple unspecified vulnerabilities in Google Chrome before 31.0.1650.48 allow attackers to execute arbitrary code or possibly have other impact via unknown vectors.
CVE-2013-3210	Opera before 12.15 does not properly block top-level domains in Set-Cookie headers, which allows remote attackers to obtain sensitive information by leveraging control of a different web site in the same top-level domain.
CVE-2013-3211	Unspecified vulnerability in Opera before 12.15 has unknown impact and attack vectors, related to a "moderately severe issue."
CVE-2013-3324	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.
CVE-2013-3325	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and

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

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

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

	CVE-2013-3337, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-3339	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-3340	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, and CVE-2013-3341.
CVE-2013-3341	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, and CVE-2013-3340.
CVE-2013-3342	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 do not properly handle operating-system domain blacklists, which has unspecified impact and attack vectors.
CVE-2013-3343	Adobe Flash Player before 10.3.183.90 and 11.x before 11.7.700.224 on Windows, before 10.3.183.90 and 11.x before 11.7.700.225 on Mac OS X, before 10.3.183.90 and 11.x before 11.2.202.291 on Linux, before 11.1.111.59 on Android 2.x and 3.x, and before 11.1.115.63 on Android 4.x; Adobe AIR before 3.7.0.2090 on Windows and Android and before 3.7.0.2100 on Mac OS X; and Adobe AIR SDK & Compiler before 3.7.0.2090 on Windows and before 3.7.0.2100 on Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.

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

CVE-2013-3363	Adobe Flash Player before 11.7.700.242 and 11.8.x before 11.8.800.168 on Windows and Mac OS X, before 11.2.202.310 on Linux, before 11.1.111.73 on Android 2.x and 3.x, and before 11.1.115.81 on Android 4.x; Adobe AIR before 3.8.0.1430; and Adobe AIR SDK & Compiler before 3.8.0.1430 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-3361, CVE-2013-3362, and CVE-2013-5324.
CVE-2013-5324	Adobe Flash Player before 11.7.700.242 and 11.8.x before 11.8.800.168 on Windows and Mac OS X, before 11.2.202.310 on Linux, before 11.1.111.73 on Android 2.x and 3.x, and before 11.1.115.81 on Android 4.x; Adobe AIR before 3.8.0.1430; and Adobe AIR SDK & Compiler before 3.8.0.1430 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-3361, CVE-2013-3362, and CVE-2013-3363.
CVE-2013-5329	Adobe Flash Player before 11.7.700.252 and 11.8.x and 11.9.x before 11.9.900.152 on Windows and Mac OS X and before 11.2.202.327 on Linux, Adobe AIR before 3.9.0.1210, Adobe AIR SDK before 3.9.0.1210, and Adobe AIR SDK & Compiler before 3.9.0.1210 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-5330.
CVE-2013-5330	Adobe Flash Player before 11.7.700.252 and 11.8.x and 11.9.x before 11.9.900.152 on Windows and Mac OS X and before 11.2.202.327 on Linux, Adobe AIR before 3.9.0.1210, Adobe AIR SDK before 3.9.0.1210, and Adobe AIR SDK & Compiler before 3.9.0.1210 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-5329.
CVE-2013-5331	Adobe Flash Player before 11.7.700.257 and 11.8.x and 11.9.x before 11.9.900.170 on Windows and Mac OS X and before 11.2.202.332 on Linux, Adobe AIR before 3.9.0.1380, Adobe AIR SDK before 3.9.0.1380, and Adobe AIR SDK & Compiler before 3.9.0.1380 allow remote attackers to execute arbitrary code via crafted .swf content that leverages an unspecified "type confusion," as exploited in the wild in December 2013.
CVE-2013-5332	Adobe Flash Player before 11.7.700.257 and 11.8.x and 11.9.x before 11.9.900.170 on Windows and Mac OS X and before 11.2.202.332 on Linux, Adobe AIR before 3.9.0.1380, Adobe AIR SDK before 3.9.0.1380, and Adobe AIR SDK & Compiler before 3.9.0.1380 allow attackers to execute arbitrary code or cause a

	denial of service (memory corruption) via unspecified vectors.
CVE-2013-6166	Google Chrome before 29 sends HTTP Cookie headers without first validating that they have the required character-set restrictions, which allows remote attackers to conduct the equivalent of a persistent Logout CSRF attack via a crafted parameter that forces a web application to set a malformed cookie within an HTTP response.
CVE-2013-6621	Use-after-free vulnerability in Google Chrome before 31.0.1650.48 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the x-webkit-speech attribute in a text INPUT element.
CVE-2013-6622	Use-after-free vulnerability in the HTMLMediaElement::didMoveToNewDocument function in core/html/HTMLMediaElement.cpp in Blink, as used in Google Chrome before 31.0.1650.48, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the movement of a media element between documents.
CVE-2013-6623	The SVG implementation in Blink, as used in Google Chrome before 31.0.1650.48, allows remote attackers to cause a denial of service (out-of-bounds read) by leveraging the use of tree order, rather than transitive dependency order, for layout.
CVE-2013-6624	Use-after-free vulnerability in Google Chrome before 31.0.1650.48 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the string values of id attributes.
CVE-2013-6625	Use-after-free vulnerability in core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 31.0.1650.48, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of DOM range objects in circumstances that require child node removal after a (1) mutation or (2) blur event.
CVE-2013-6626	The WebContentsImpl::AttachInterstitialPage function in content/browser/web_contents/web_contents_impl.cc in Google Chrome before 31.0.1650.48 does not cancel JavaScript dialogs upon generating an interstitial warning, which allows remote attackers to spoof the address bar via a crafted web site.
CVE-2013-6627	net/http/http_stream_parser.cc in Google Chrome before 31.0.1650.48 does not properly process HTTP Informational (aka 1xx) status codes, which allows remote web servers to cause a denial of service (out-of-bounds read) via a crafted response.

CVE-2013-6628	net/socket/ssl_client_socket_nss.cc in the TLS implementation in Google Chrome before 31.0.1650.48 does not ensure that a server's X.509 certificate is the same during renegotiation as it was before renegotiation, which might allow remote web servers to interfere with trust relationships by renegotiating a session.
CVE-2013-6629	The get_sos function in jdmarker.c in (1) libjpeg 6b and (2) libjpeg-turbo through 1.3.0, as used in Google Chrome before 31.0.1650.48, Ghostscript, and other products, does not check for certain duplications of component data during the reading of segments that follow Start Of Scan (SOS) JPEG markers, which allows remote attackers to obtain sensitive information from uninitialized memory locations via a crafted JPEG image.
CVE-2013-6630	The get_dht function in jdmarker.c in libjpeg-turbo through 1.3.0, as used in Google Chrome before 31.0.1650.48 and other products, does not set all elements of a certain Huffman value array during the reading of segments that follow Define Huffman Table (DHT) JPEG markers, which allows remote attackers to obtain sensitive information from uninitialized memory locations via a crafted JPEG image.
CVE-2013-6631	Use-after-free vulnerability in the Channel::SendRTCPPacket function in voice_engine/channel.cc in libjingle in WebRTC, as used in Google Chrome before 31.0.1650.48 and other products, allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via vectors that trigger the absence of certain statistics initialization, leading to the skipping of a required DeRegisterExternalTransport call.
CVE-2013-6632	Integer overflow in Google Chrome before 31.0.1650.57 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as demonstrated during a Mobile Pwn2Own competition at PacSec 2013.
CVE-2013-6634	The OneClickSigninHelper::ShowInfoBarIfPossible function in browser/ui/sync/one_click_signin_helper.cc in Google Chrome before 31.0.1650.63 uses an incorrect URL during realm validation, which allows remote attackers to conduct session fixation attacks and hijack web sessions by triggering improper sync after a 302 (aka Found) HTTP status code.
CVE-2013-6635	Use-after-free vulnerability in the editing implementation in Blink, as used in Google Chrome before 31.0.1650.63, allows remote attackers to cause a denial of service or possibly have unspecified other impact via JavaScript code that triggers removal of a node during processing of the DOM

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

CVE-2013-6644	Multiple unspecified vulnerabilities in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-6645	Use-after-free vulnerability in the OnWindowRemovingFromRootWindow function in content/browser/web_contents/web_contents_view_aura.cc in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving certain print-preview and tab-switch actions that interact with a speech input element.
CVE-2013-6646	Use-after-free vulnerability in the Web Workers implementation in Google Chrome before 32.0.1700.76 on Windows and before 32.0.1700.77 on Mac OS X and Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the shutting down of a worker process.
CVE-2013-6649	Use-after-free vulnerability in the RenderSVGImage::paint function in core/rendering/svg/RenderSVGImage.cpp in Blink, as used in Google Chrome before 32.0.1700.102, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a zero-size SVG image.
CVE-2013-6650	The StoreBuffer::ExemptPopularPages function in store-buffer.cc in Google V8 before 3.22.24.16, as used in Google Chrome before 32.0.1700.102, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via vectors that trigger incorrect handling of "popular pages."
CVE-2013-6653	Use-after-free vulnerability in the web contents implementation in Google Chrome before 33.0.1750.117 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving attempted conflicting access to the color chooser.
CVE-2013-6654	The SVGAnimateElement::calculateAnimatedValue function in core/svg/SVGAnimateElement.cpp in Blink, as used in Google Chrome before 33.0.1750.117, does not properly handle unexpected data types, which allows remote attackers to cause a denial of service (incorrect cast) or possibly have unspecified other impact via unknown vectors.

CVE-2013-6655	Use-after-free vulnerability in Blink, as used in Google Chrome before 33.0.1750.117, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to improper handling of overflowchanged DOM events during interaction between JavaScript and layout.
CVE-2013-6656	The XSSAuditor::init function in core/html/parser/XSSAuditor.cpp in the XSS auditor in Blink, as used in Google Chrome before 33.0.1750.117, processes POST requests by using the body of a redirecting page instead of the body of a redirect target, which allows remote attackers to obtain sensitive information via unspecified vectors.
CVE-2013-6657	core/html/parser/XSSAuditor.cpp in the XSS auditor in Blink, as used in Google Chrome before 33.0.1750.117, inserts the about:blank URL during certain blocking of FORM elements within HTTP requests, which allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via unspecified vectors.
CVE-2013-6658	Multiple use-after-free vulnerabilities in the layout implementation in Blink, as used in Google Chrome before 33.0.1750.117, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving (1) running JavaScript code during execution of the updateWidgetPositions function or (2) making a call into a plugin during execution of the updateWidgetPositions function.
CVE-2013-6659	The SSLClientSocketNSS::Core::OwnAuthCertHandler function in net/socket/ssl_client_socket_nss.cc in Google Chrome before 33.0.1750.117 does not prevent changes to server X.509 certificates during renegotiations, which allows remote SSL servers to trigger use of a new certificate chain, inconsistent with the user's expectations, by initiating a TLS renegotiation.
CVE-2013-6660	The drag-and-drop implementation in Google Chrome before 33.0.1750.117 does not properly restrict the information in WebDropData data structures, which allows remote attackers to discover full pathnames via a crafted web site.
CVE-2013-6661	Multiple unspecified vulnerabilities in Google Chrome before 33.0.1750.117 allow attackers to bypass the sandbox protection mechanism after obtaining renderer access, or have other impact, via unknown vectors.
CVE-2013-6663	Use-after-free vulnerability in the SVGImage::setContainerSize function in core/svg/graphics/SVGImage.cpp in the SVG implementation in Blink, as used in Google Chrome before 33.0.1750.146, allows remote attackers to cause a denial of service

	or possibly have unspecified other impact via vectors related to the resizing of a view.
CVE-2013-6664	Use-after-free vulnerability in the FormAssociatedElement::formRemovedFromTree function in core/html/FormAssociatedElement.cpp in Blink, as used in Google Chrome before 33.0.1750.146, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving FORM elements, as demonstrated by use of the speech-recognition feature.
CVE-2013-6665	Heap-based buffer overflow in the ResourceProvider::InitializeSoftware function in cc/resources/resource_provider.cc in Google Chrome before 33.0.1750.146 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large texture size that triggers improper memory allocation in the software renderer.
CVE-2013-6666	The PepperFlashRendererHost::OnNavigate function in renderer/pepper/pepper_flash_renderer_host.cc in Google Chrome before 33.0.1750.146 does not verify that all headers are Cross-Origin Resource Sharing (CORS) simple headers before proceeding with a PPB_Flash.Navigate operation, which might allow remote attackers to bypass intended CORS restrictions via an inappropriate header.
CVE-2013-6667	Multiple unspecified vulnerabilities in Google Chrome before 33.0.1750.146 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-6668	Multiple unspecified vulnerabilities in Google V8 before 3.24.35.10, as used in Google Chrome before 33.0.1750.146, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-6802	Google Chrome before 31.0.1650.57 allows remote attackers to bypass intended sandbox restrictions by leveraging access to a renderer process, as demonstrated during a Mobile Pwn2Own competition at PacSec 2013, a different vulnerability than CVE-2013-6632.
CVE-2013-6886	RealVNC VNC 5.0.6 on Mac OS X, Linux, and UNIX allows local users to gain privileges via a crafted argument to the (1) vncserver, (2) vncserver-x11, or (3) Xvnc helper.
CVE-2014-0491	Adobe Flash Player before 11.7.700.260 and 11.8.x and 11.9.x before 12.0.0.38 on Windows and Mac OS X and before 11.2.202.335 on Linux, Adobe AIR before 4.0.0.1390, Adobe AIR SDK before 4.0.0.1390, and Adobe AIR SDK & Compiler before 4.0.0.1390 allow

	attackers to bypass unspecified protection mechanisms via unknown vectors.
CVE-2014-0492	Adobe Flash Player before 11.7.700.260 and 11.8.x and 11.9.x before 12.0.0.38 on Windows and Mac OS X and before 11.2.202.335 on Linux, Adobe AIR before 4.0.0.1390, Adobe AIR SDK before 4.0.0.1390, and Adobe AIR SDK & Compiler before 4.0.0.1390 allow attackers to defeat the ASLR protection mechanism by leveraging an "address leak."
CVE-2014-0497	Integer underflow in Adobe Flash Player before 11.7.700.261 and 11.8.x through 12.0.x before 12.0.0.44 on Windows and Mac OS X, and before 11.2.202.336 on Linux, allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2014-0498	Stack-based buffer overflow in Adobe Flash Player before 11.7.700.269 and 11.8.x through 12.0.x before 12.0.0.70 on Windows and Mac OS X and before 11.2.202.341 on Linux, Adobe AIR before 4.0.0.1628 on Android, Adobe AIR SDK before 4.0.0.1628, and Adobe AIR SDK & Compiler before 4.0.0.1628 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2014-0499	Adobe Flash Player before 11.7.700.269 and 11.8.x through 12.0.x before 12.0.0.70 on Windows and Mac OS X and before 11.2.202.341 on Linux, Adobe AIR before 4.0.0.1628 on Android, Adobe AIR SDK before 4.0.0.1628, and Adobe AIR SDK & Compiler before 4.0.0.1628 do not prevent access to address information, which makes it easier for attackers to bypass the ASLR protection mechanism via unspecified vectors.
CVE-2014-0502	Double free vulnerability in Adobe Flash Player before 11.7.700.269 and 11.8.x through 12.0.x before 12.0.0.70 on Windows and Mac OS X and before 11.2.202.341 on Linux, Adobe AIR before 4.0.0.1628 on Android, Adobe AIR SDK before 4.0.0.1628, and Adobe AIR SDK & Compiler before 4.0.0.1628 allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in February 2014.
CVE-2014-0503	Adobe Flash Player before 11.7.700.272 and 11.8.x through 12.0.x before 12.0.0.77 on Windows and OS X, and before 11.2.202.346 on Linux, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2014-0504	Adobe Flash Player before 11.7.700.272 and 11.8.x through 12.0.x before 12.0.0.77 on Windows and OS X, and before 11.2.202.346 on Linux, allows attackers to read the clipboard via unspecified vectors.
CVE-2014-0506	Use-after-free vulnerability in Adobe Flash Player before 11.7.700.275 and 11.8.x through 13.0.x before 13.0.0.182 on Windows and OS X and before

	11.2.202.350 on Linux, Adobe AIR before 13.0.0.83 on Android, Adobe AIR SDK before 13.0.0.83, and Adobe AIR SDK & Compiler before 13.0.0.83 allows remote attackers to execute arbitrary code, and possibly bypass an Internet Explorer sandbox protection mechanism, via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2014.
CVE-2014-0507	Buffer overflow in Adobe Flash Player before 11.7.700.275 and 11.8.x through 13.0.x before 13.0.0.182 on Windows and OS X and before 11.2.202.350 on Linux, Adobe AIR before 13.0.0.83 on Android, Adobe AIR SDK before 13.0.0.83, and Adobe AIR SDK & Compiler before 13.0.0.83 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2014-0508	Adobe Flash Player before 11.7.700.275 and 11.8.x through 13.0.x before 13.0.0.182 on Windows and OS X and before 11.2.202.350 on Linux, Adobe AIR before 13.0.0.83 on Android, Adobe AIR SDK before 13.0.0.83, and Adobe AIR SDK & Compiler before 13.0.0.83 allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors.
CVE-2014-0509	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 11.7.700.275 and 11.8.x through 13.0.x before 13.0.0.182 on Windows and OS X and before 11.2.202.350 on Linux, Adobe AIR before 13.0.0.83 on Android, Adobe AIR SDK before 13.0.0.83, and Adobe AIR SDK & Compiler before 13.0.0.83 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2014-0515	Buffer overflow in Adobe Flash Player before 11.7.700.279 and 11.8.x through 13.0.x before 13.0.0.206 on Windows and OS X, and before 11.2.202.356 on Linux, allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in April 2014.
CVE-2014-0516	Adobe Flash Player before 13.0.0.214 on Windows and OS X and before 11.2.202.359 on Linux, Adobe AIR SDK before 13.0.0.111, and Adobe AIR SDK & Compiler before 13.0.0.111 allow remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2014-0517	Adobe Flash Player before 13.0.0.214 on Windows and OS X and before 11.2.202.359 on Linux, Adobe AIR SDK before 13.0.0.111, and Adobe AIR SDK & Compiler before 13.0.0.111 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0518, CVE-2014-0519, and CVE-2014-0520.
CVE-2014-0518	Adobe Flash Player before 13.0.0.214 on Windows and OS X and before 11.2.202.359 on Linux, Adobe

	AIR SDK before 13.0.0.111, and Adobe AIR SDK & Compiler before 13.0.0.111 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0517, CVE-2014-0519, and CVE-2014-0520.
CVE-2014-0519	Adobe Flash Player before 13.0.0.214 on Windows and OS X and before 11.2.202.359 on Linux, Adobe AIR SDK before 13.0.0.111, and Adobe AIR SDK & Compiler before 13.0.0.111 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0517, CVE-2014-0518, and CVE-2014-0520.
CVE-2014-0520	Adobe Flash Player before 13.0.0.214 on Windows and OS X and before 11.2.202.359 on Linux, Adobe AIR SDK before 13.0.0.111, and Adobe AIR SDK & Compiler before 13.0.0.111 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0517, CVE-2014-0518, and CVE-2014-0519.
CVE-2014-0531	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2014-0532 and CVE-2014-0533.
CVE-2014-0532	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2014-0531 and CVE-2014-0533.
CVE-2014-0533	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2014-0531 and CVE-2014-0532.
CVE-2014-0534	Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0535.

CVE-2014-0535	Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0534.
CVE-2014-0536	Adobe Flash Player before 13.0.0.223 and 14.x before 14.0.0.125 on Windows and OS X and before 11.2.202.378 on Linux, Adobe AIR before 14.0.0.110, Adobe AIR SDK before 14.0.0.110, and Adobe AIR SDK & Compiler before 14.0.0.110 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2014-0537	Adobe Flash Player before 13.0.0.231 and 14.x before 14.0.0.145 on Windows and OS X and before 11.2.202.394 on Linux, Adobe AIR before 14.0.0.137 on Android, Adobe AIR SDK before 14.0.0.137, and Adobe AIR SDK & Compiler before 14.0.0.137 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0539.
CVE-2014-0538	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2014-0539	Adobe Flash Player before 13.0.0.231 and 14.x before 14.0.0.145 on Windows and OS X and before 11.2.202.394 on Linux, Adobe AIR before 14.0.0.137 on Android, Adobe AIR SDK before 14.0.0.137, and Adobe AIR SDK & Compiler before 14.0.0.137 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2014-0537.
CVE-2014-0540	Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors, a different vulnerability than CVE-2014-0542, CVE-2014-0543, CVE-2014-0544, and CVE-2014-0545.
CVE-2014-0541	Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android,

	Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 allow attackers to bypass intended access restrictions via unspecified vectors.
CVE-2014-0542	Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors, a different vulnerability than CVE-2014-0540, CVE-2014-0543, CVE-2014-0544, and CVE-2014-0545.
CVE-2014-0543	Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors, a different vulnerability than CVE-2014-0540, CVE-2014-0542, CVE-2014-0544, and CVE-2014-0545.
CVE-2014-0544	Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors, a different vulnerability than CVE-2014-0540, CVE-2014-0542, CVE-2014-0543, and CVE-2014-0545.
CVE-2014-0545	Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors, a different vulnerability than CVE-2014-0540, CVE-2014-0542, CVE-2014-0543, and CVE-2014-0544.
CVE-2014-0547	Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR

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

	X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0547, CVE-2014-0549, CVE-2014-0550, CVE-2014-0551, and CVE-2014-0555.
CVE-2014-0553	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2014-0554	Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allow attackers to bypass intended access restrictions via unspecified vectors.
CVE-2014-0555	Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0547, CVE-2014-0549, CVE-2014-0550, CVE-2014-0551, and CVE-2014-0552.
CVE-2014-0556	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before 15.0.0.249 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-0559.
CVE-2014-0557	Adobe Flash Player before 13.0.0.244 and 14.x and 15.x before 15.0.0.152 on Windows and OS X and before 11.2.202.406 on Linux, Adobe AIR before 15.0.0.249 on Windows and OS X and before 15.0.0.252 on Android, Adobe AIR SDK before 15.0.0.249, and Adobe AIR SDK & Compiler before

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

CVE-2014-0576	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0581, CVE-2014-8440, and CVE-2014-8441.
CVE-2014-0577	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2014-0584, CVE-2014-0585, CVE-2014-0586, and CVE-2014-0590.
CVE-2014-0578	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-3115, CVE-2015-3116, CVE-2015-3125, and CVE-2015-5116.
CVE-2014-0580	Adobe Flash Player before 13.0.0.259 and 14.x through 16.x before 16.0.0.235 on Windows and OS X and before 11.2.202.425 on Linux allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2014-0581	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0576, CVE-2014-8440, and CVE-2014-8441.
CVE-2014-0582	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-0589.
CVE-2014-0583	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223

	on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allows attackers to complete a transition from Low Integrity to Medium Integrity via unspecified vectors.
CVE-2014-0584	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2014-0577, CVE-2014-0585, CVE-2014-0586, and CVE-2014-0590.
CVE-2014-0585	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2014-0577, CVE-2014-0584, CVE-2014-0586, and CVE-2014-0590.
CVE-2014-0586	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2014-0577, CVE-2014-0584, CVE-2014-0585, and CVE-2014-0590.
CVE-2014-0587	Adobe Flash Player before 13.0.0.259 and 14.x through 16.x before 16.0.0.235 on Windows and OS X and before 11.2.202.425 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-9164.
CVE-2014-0588	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-0573 and CVE-2014-8438.
CVE-2014-0589	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK

	before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-0582.
CVE-2014-0590	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2014-0577, CVE-2014-0584, CVE-2014-0585, and CVE-2014-0586.
CVE-2014-1681	Multiple unspecified vulnerabilities in Google Chrome before 32.0.1700.102 have unknown impact and attack vectors, related to 12 "security fixes [that were not] either contributed by external researchers or particularly interesting."
CVE-2014-1700	Use-after-free vulnerability in modules/speech/SpeechSynthesis.cpp in Blink, as used in Google Chrome before 33.0.1750.149, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of a certain utterance data structure.
CVE-2014-1701	The GenerateFunction function in bindings/scripts/code_generator_v8.pm in Blink, as used in Google Chrome before 33.0.1750.149, does not implement a certain cross-origin restriction for the EventTarget::dispatchEvent function, which allows remote attackers to conduct Universal XSS (UXSS) attacks via vectors involving events.
CVE-2014-1702	Use-after-free vulnerability in the DatabaseThread::cleanupDatabaseThread function in modules/webdatabase/DatabaseThread.cpp in the web database implementation in Blink, as used in Google Chrome before 33.0.1750.149, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of scheduled tasks during shutdown of a thread.
CVE-2014-1703	Use-after-free vulnerability in the WebSocketDispatcherHost::SendOrDrop function in content/browser/renderer_host/websocket_dispatcher_host.cc in the Web Sockets implementation in Google Chrome before 33.0.1750.149 might allow remote attackers to bypass the sandbox protection mechanism by leveraging an incorrect deletion in a certain failure case.
CVE-2014-1704	Multiple unspecified vulnerabilities in Google V8 before 3.23.17.18, as used in Google Chrome before 33.0.1750.149, allow attackers to cause a denial of

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

CVE-2014-1719	Use-after-free vulnerability in the WebSharedWorkerStub::OnTerminateWorkerContext function in content/worker/websharedworker_stub.cc in the Web Workers implementation in Google Chrome before 34.0.1847.116 allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via vectors that trigger a SharedWorker termination during script loading.
CVE-2014-1720	Use-after-free vulnerability in the HTMLBodyElement::insertedInto function in core/html/HTMLBodyElement.cpp in Blink, as used in Google Chrome before 34.0.1847.116, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving attributes.
CVE-2014-1721	Google V8, as used in Google Chrome before 34.0.1847.116, does not properly implement lazy deoptimization, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code, as demonstrated by improper handling of a heap allocation of a number outside the Small Integer (aka smi) range.
CVE-2014-1722	Use-after-free vulnerability in the RenderBlock::addChildIgnoringAnonymousColumnBlocks function in core/rendering/RenderBlock.cpp in Blink, as used in Google Chrome before 34.0.1847.116, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving addition of a child node.
CVE-2014-1723	The UnescapeURLWithOffsetsImpl function in net/base/escape.cc in Google Chrome before 34.0.1847.116 does not properly handle bidirectional Internationalized Resource Identifiers (IRIs), which makes it easier for remote attackers to spoof URLs via crafted use of right-to-left (RTL) Unicode text.
CVE-2014-1724	Use-after-free vulnerability in Free(b)soft Laboratory Speech Dispatcher 0.7.1, as used in Google Chrome before 34.0.1847.116, allows remote attackers to cause a denial of service (application hang) or possibly have unspecified other impact via a text-to-speech request.
CVE-2014-1725	The base64DecodeInternal function in wtf/text/Base64.cpp in Blink, as used in Google Chrome before 34.0.1847.116, does not properly handle string data composed exclusively of whitespace characters, which allows remote attackers to cause a denial of service (out-of-bounds read) via a window.atob method call.
CVE-2014-1726	The drag implementation in Google Chrome before 34.0.1847.116 allows user-assisted remote attackers

	to bypass the Same Origin Policy and forge local pathnames by leveraging renderer access.
CVE-2014-1727	Use-after-free vulnerability in content/renderer/renderer_webcolorchooser_impl.h in Google Chrome before 34.0.1847.116 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to forms.
CVE-2014-1728	Multiple unspecified vulnerabilities in Google Chrome before 34.0.1847.116 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-1729	Multiple unspecified vulnerabilities in Google V8 before 3.24.35.22, as used in Google Chrome before 34.0.1847.116, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-1730	Google V8, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, does not properly store internationalization metadata, which allows remote attackers to bypass intended access restrictions by leveraging "type confusion" and reading property values, related to i18n.js and runtime.cc.
CVE-2014-1731	core/html/HTMLSelectElement.cpp in the DOM implementation in Blink, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, does not properly check renderer state upon a focus event, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion" for SELECT elements.
CVE-2014-1732	Use-after-free vulnerability in browser/ui/views/speech_recognition_bubble_views.cc in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact via an INPUT element that triggers the presence of a Speech Recognition Bubble window for an incorrect duration.
CVE-2014-1733	The PointerCompare function in codegen.cc in Seccomp-BPF, as used in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux, does not properly merge blocks, which might allow remote attackers to bypass intended sandbox restrictions by leveraging renderer access.
CVE-2014-1734	Multiple unspecified vulnerabilities in Google Chrome before 34.0.1847.131 on Windows and OS X and before 34.0.1847.132 on Linux allow attackers to cause

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

CVE-2014-1745	Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger removal of an SVGFontFaceElement object, related to core/svg/SVGFontFaceElement.cpp.
CVE-2014-1746	The InMemoryUrlProtocol::Read function in media/filters/in_memory_url_protocol.cc in Google Chrome before 35.0.1916.114 relies on an insufficiently large integer data type, which allows remote attackers to cause a denial of service (out-of-bounds read) via vectors that trigger use of a large buffer.
CVE-2014-1747	Cross-site scripting (XSS) vulnerability in the DocumentLoader::maybeCreateArchive function in core/loader/DocumentLoader.cpp in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to inject arbitrary web script or HTML via crafted MHTML content, aka "Universal XSS (UXSS)."
CVE-2014-1748	The ScrollView::paint function in platform/scroll/ScrollView.cpp in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to spoof the UI by extending scrollbar painting into the parent frame.
CVE-2014-1749	Multiple unspecified vulnerabilities in Google Chrome before 35.0.1916.114 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3120	The default configuration in Elasticsearch before 1.2 enables dynamic scripting, which allows remote attackers to execute arbitrary MVEL expressions and Java code via the source parameter to _search. NOTE: this only violates the vendor's intended security policy if the user does not run Elasticsearch in its own independent virtual machine.
CVE-2014-3152	Integer underflow in the LCodeGen::PrepareKeyedOperand function in arm/lithium-codegen-arm.cc in Google V8 before 3.25.28.16, as used in Google Chrome before 35.0.1916.114, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a negative key value.
CVE-2014-3154	Use-after-free vulnerability in the ChildThread::Shutdown function in content/child/child_thread.cc in the filesystem API in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to a Blink shutdown.
CVE-2014-3155	net/spdy/spdy_write_queue.cc in the SPDY implementation in Google Chrome before

	35.0.1916.153 allows remote attackers to cause a denial of service (out-of-bounds read) by leveraging incorrect queue maintenance.
CVE-2014-3156	Buffer overflow in the clipboard implementation in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger unexpected bitmap data, related to content/renderer/renderer_clipboard_client.cc and content/renderer/webclipboard_impl.cc.
CVE-2014-3157	Heap-based buffer overflow in the FFmpegVideoDecoder::GetVideoBuffer function in media/filters/ffmpeg_video_decoder.cc in Google Chrome before 35.0.1916.153 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging VideoFrame data structures that are too small for proper interaction with an underlying FFmpeg library.
CVE-2014-3160	The ResourceFetcher::canRequest function in core/fetch/ResourceFetcher.cpp in Blink, as used in Google Chrome before 36.0.1985.125, does not properly restrict subresource requests associated with SVG files, which allows remote attackers to bypass the Same Origin Policy via a crafted file.
CVE-2014-3162	Multiple unspecified vulnerabilities in Google Chrome before 36.0.1985.125 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3165	Use-after-free vulnerability in modules/websockets/WorkerThreadableWebSocketChannel.cpp in the Web Sockets implementation in Blink, as used in Google Chrome before 36.0.1985.143, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an unexpectedly long lifetime of a temporary object during method completion.
CVE-2014-3166	The Public Key Pinning (PKP) implementation in Google Chrome before 36.0.1985.143 on Windows, OS X, and Linux, and before 36.0.1985.135 on Android, does not correctly consider the properties of SPDY connections, which allows remote attackers to obtain sensitive information by leveraging the use of multiple domain names.
CVE-2014-3167	Multiple unspecified vulnerabilities in Google Chrome before 36.0.1985.143 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3168	Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before 37.0.2062.94, allows remote attackers to cause a denial

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

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

CVE-2014-3192	Use-after-free vulnerability in the ProcessingInstruction::setXSLStyleSheet function in core/dom/ProcessingInstruction.cpp in the DOM implementation in Blink, as used in Google Chrome before 38.0.2125.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-3193	The SessionService::GetLastSession function in browser/sessions/session_service.cc in Google Chrome before 38.0.2125.101 allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors that leverage "type confusion" for callback processing.
CVE-2014-3194	Use-after-free vulnerability in the Web Workers implementation in Google Chrome before 38.0.2125.101 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-3195	Google V8, as used in Google Chrome before 38.0.2125.101, does not properly track JavaScript heap-memory allocations as allocations of uninitialized memory and does not properly concatenate arrays of double-precision floating-point numbers, which allows remote attackers to obtain sensitive information via crafted JavaScript code, related to the PagedSpace::AllocateRaw and NewSpace::AllocateRaw functions in heap/spaces-inl.h, the LargeObjectSpace::AllocateRaw function in heap/spaces.cc, and the Runtime_ArrayConcat function in runtime.cc.
CVE-2014-3196	base/memory/shared_memory_win.cc in Google Chrome before 38.0.2125.101 on Windows does not properly implement read-only restrictions on shared memory, which allows attackers to bypass a sandbox protection mechanism via unspecified vectors.
CVE-2014-3197	The NavigationScheduler::schedulePageBlock function in core/loader/NavigationScheduler.cpp in Blink, as used in Google Chrome before 38.0.2125.101, does not properly provide substitute data for pages blocked by the XSS auditor, which allows remote attackers to obtain sensitive information via a crafted web site.
CVE-2014-3198	The Instance::HandleInputEvent function in pdf/instance.cc in the PDFium component in Google Chrome before 38.0.2125.101 interprets a certain -1 value as an index instead of a no-visible-page error code, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2014-3199	The wrap function in bindings/core/v8/custom/V8EventCustom.cpp in the V8 bindings in Blink, as used in Google Chrome before 38.0.2125.101, has

	an erroneous fallback outcome for wrapper-selection failures, which allows remote attackers to cause a denial of service via vectors that trigger stopping a worker process that had been handling an Event object.
CVE-2014-3200	Multiple unspecified vulnerabilities in Google Chrome before 38.0.2125.101 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3803	The SpeechInput feature in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to enable microphone access and obtain speech-recognition text without indication via an INPUT element with a -x-webkit-speech attribute.
CVE-2014-4671	Adobe Flash Player before 13.0.0.231 and 14.x before 14.0.0.145 on Windows and OS X and before 11.2.202.394 on Linux, Adobe AIR before 14.0.0.137 on Android, Adobe AIR SDK before 14.0.0.137, and Adobe AIR SDK & Compiler before 14.0.0.137 do not properly restrict the SWF file format, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks against JSONP endpoints, and obtain sensitive information, via a crafted OBJECT element with SWF content satisfying the character-set requirements of a callback API.
CVE-2014-5333	Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 do not properly restrict the SWF file format, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks against JSONP endpoints, and obtain sensitive information, via a crafted OBJECT element with SWF content satisfying the character-set requirements of a callback API, in conjunction with a manipulation involving a '$' (dollar sign) or '(' (open parenthesis) character. NOTE: this issue exists because of an incomplete fix for CVE-2014-4671.
CVE-2014-7899	Google Chrome before 38.0.2125.101 allows remote attackers to spoof the address bar by placing a blob: substring at the beginning of the URL, followed by the original URI scheme and a long username string.
CVE-2014-7900	Use-after-free vulnerability in the CPDF_Parser::IsLinearizedFile function in fpdfapi/fpdf_parser/fpdf_parser_parser.cpp in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.
CVE-2014-7901	Integer overflow in the opj_t2_read_packet_data function in fxcodec/fx_libopenjpeg/libopenjpeg20/t2.c

	in OpenJPEG in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long segment in a JPEG image.
CVE-2014-7902	Use-after-free vulnerability in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.
CVE-2014-7903	Buffer overflow in OpenJPEG before r2911 in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted JPEG image.
CVE-2014-7904	Buffer overflow in Skia, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-7906	Use-after-free vulnerability in the Pepper plugins in Google Chrome before 39.0.2171.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted Flash content that triggers an attempted PepperMediaDeviceManager access outside of the object's lifetime.
CVE-2014-7907	Multiple use-after-free vulnerabilities in modules/screen_orientation/ScreenOrientationController.cpp in Blink, as used in Google Chrome before 39.0.2171.65, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger improper handling of a detached frame, related to the (1) lock and (2) unlock methods.
CVE-2014-7908	Multiple integer overflows in the CheckMov function in media/base/container_names.cc in Google Chrome before 39.0.2171.65 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a large atom in (1) MPEG-4 or (2) QuickTime .mov data.
CVE-2014-7909	effects/SkDashPathEffect.cpp in Skia, as used in Google Chrome before 39.0.2171.65, computes a hash key using uninitialized integer values, which might allow remote attackers to cause a denial of service by rendering crafted data.
CVE-2014-7910	Multiple unspecified vulnerabilities in Google Chrome before 39.0.2171.65 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-7923	The Regular Expressions package in International Components for Unicode (ICU) 52 before SVN revision 292944, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (memory corruption) or possibly have

	unspecified other impact via vectors related to a look-behind expression.
CVE-2014-7924	Use-after-free vulnerability in the IndexedDB implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering duplicate BLOB references, related to content/browser/indexed_db/indexed_db_callbacks.cc and content/browser/indexed_db/indexed_db_dispatcher_host.cc.
CVE-2014-7925	Use-after-free vulnerability in the WebAudio implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an audio-rendering thread in which AudioNode data is improperly maintained.
CVE-2014-7926	The Regular Expressions package in International Components for Unicode (ICU) 52 before SVN revision 292944, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via vectors related to a zero-length quantifier.
CVE-2014-7927	The SimplifiedLowering::DoLoadBuffer function in compiler/simplified-lowering.cc in Google V8, as used in Google Chrome before 40.0.2214.91, does not properly choose an integer data type, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2014-7928	hydrogen.cc in Google V8, as used Google Chrome before 40.0.2214.91, does not properly handle arrays with holes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code that triggers an array copy.
CVE-2014-7929	Use-after-free vulnerability in the HTMLScriptElement::didMoveToNewDocument function in core/html/HTMLScriptElement.cpp in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving movement of a SCRIPT element across documents.
CVE-2014-7930	Use-after-free vulnerability in core/events/TreeScopeEventContext.cpp in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified

	other impact via crafted JavaScript code that triggers improper maintenance of TreeScope data.
CVE-2014-7931	factory.cc in Google V8, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code that triggers improper maintenance of backing-store pointers.
CVE-2014-7932	Use-after-free vulnerability in the Element::detach function in core/dom/Element.cpp in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving pending updates of detached elements.
CVE-2014-7933	Use-after-free vulnerability in the matroska_read_seek function in libavformat/matroskadec.c in FFmpeg before 2.5.1, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Matroska file that triggers improper maintenance of tracks data.
CVE-2014-7934	Use-after-free vulnerability in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to unexpected absence of document data structures.
CVE-2014-7935	Use-after-free vulnerability in browser/speech/tts_message_filter.cc in the Speech implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving utterances from a closed tab.
CVE-2014-7936	Use-after-free vulnerability in the ZoomBubbleView::Close function in browser/ui/views/location_bar/zoom_bubble_view.cc in the Views implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document that triggers improper maintenance of a zoom bubble.
CVE-2014-7937	Multiple off-by-one errors in libavcodec/vorbisdec.c in FFmpeg before 2.4.2, as used in Google Chrome before 40.0.2214.91, allow remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted Vorbis I data.
CVE-2014-7938	The Fonts implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a

	denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2014-7939	Google Chrome before 40.0.2214.91, when the Harmony proxy in Google V8 is enabled, allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code with Proxy.create and console.log calls, related to HTTP responses that lack an "X-Content-Type-Options: nosniff" header.
CVE-2014-7940	The collator implementation in i18n/ucol.cpp in International Components for Unicode (ICU) 52 through SVN revision 293126, as used in Google Chrome before 40.0.2214.91, does not initialize memory for a data structure, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted character sequence.
CVE-2014-7941	The SelectionOwner::ProcessTarget function in ui/base/x/selection_owner.cc in the UI implementation in Google Chrome before 40.0.2214.91 uses an incorrect data type for a certain length value, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted X11 data.
CVE-2014-7942	The Fonts implementation in Google Chrome before 40.0.2214.91 does not initialize memory for a data structure, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-7943	Skia, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2014-7944	The sycc422_to_rgb function in fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 40.0.2214.91, does not properly handle odd values of image width, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document.
CVE-2014-7945	OpenJPEG before r2908, as used in PDFium in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document, related to j2k.c, jp2.c, and t2.c.
CVE-2014-7946	The RenderTable::simplifiedNormalFlowLayout function in core/rendering/RenderTable.cpp in Blink, as used in Google Chrome before 40.0.2214.91, skips captions during table layout in certain situations, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors related to the Fonts implementation.
CVE-2014-7947	OpenJPEG before r2944, as used in PDFium in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via a

	crafted PDF document, related to j2k.c, jp2.c, pi.c, t1.c, t2.c, and tcd.c.
CVE-2014-7948	The AppCacheUpdateJob::URLFetcher::OnResponseStarted function in content/browser/appcache/appcache_update_job.cc in Google Chrome before 40.0.2214.91 proceeds with AppCache caching for SSL sessions even if there is an X.509 certificate error, which allows man-in-the-middle attackers to spoof HTML5 application content via a crafted certificate.
CVE-2014-7967	Multiple unspecified vulnerabilities in Google V8 before 3.28.71.15, as used in Google Chrome before 38.0.2125.101, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-8437	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow remote attackers to discover session tokens via unspecified vectors.
CVE-2014-8438	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-0573 and CVE-2014-0588.
CVE-2014-8439	Adobe Flash Player before 13.0.0.258 and 14.x and 15.x before 15.0.0.239 on Windows and OS X and before 11.2.202.424 on Linux, Adobe AIR before 15.0.0.293, Adobe AIR SDK before 15.0.0.302, and Adobe AIR SDK & Compiler before 15.0.0.302 allow attackers to execute arbitrary code or cause a denial of service (invalid pointer dereference) via unspecified vectors.
CVE-2014-8440	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0576, CVE-2014-0581, and CVE-2014-8441.
CVE-2014-8441	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356,

	and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0576, CVE-2014-0581, and CVE-2014-8440.
CVE-2014-8442	Adobe Flash Player before 13.0.0.252 and 14.x and 15.x before 15.0.0.223 on Windows and OS X and before 11.2.202.418 on Linux, Adobe AIR before 15.0.0.356, Adobe AIR SDK before 15.0.0.356, and Adobe AIR SDK & Compiler before 15.0.0.356 allow attackers to complete a transition from Low Integrity to Medium Integrity by leveraging incorrect permissions.
CVE-2014-8443	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.259 and 14.x through 16.x before 16.0.0.235 on Windows and OS X and before 11.2.202.425 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2014-9092	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-2014-9162	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-2014-9620	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-2014-9646	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-2014-9689	content/renderer/device_sensors/ device_orientation_event_pump.cc in Google Chrome before 41.0.2272.76 does not properly restrict access to high-rate gyroscope data, which makes it easier for remote attackers to obtain speech signals from a device's physical environment via a crafted web site that listens for ondeviceorientation events, a different vulnerability than CVE-2015-1231.
CVE-2015-0301	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 do not properly validate files, which has unspecified impact and attack vectors.
CVE-2015-0302	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allow attackers to obtain sensitive keystroke information via unspecified vectors.
CVE-2015-0303	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and

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

CVE-2015-0309	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0304.
CVE-2015-0310	Adobe Flash Player before 13.0.0.262 and 14.x through 16.x before 16.0.0.287 on Windows and OS X and before 11.2.202.438 on Linux does not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism on Windows, and have an unspecified impact on other platforms, via unknown vectors, as exploited in the wild in January 2015.
CVE-2015-0311	Unspecified vulnerability in Adobe Flash Player through 13.0.0.262 and 14.x, 15.x, and 16.x through 16.0.0.287 on Windows and OS X and through 11.2.202.438 on Linux allows remote attackers to execute arbitrary code via unknown vectors, as exploited in the wild in January 2015.
CVE-2015-0312	Double free vulnerability in Adobe Flash Player before 13.0.0.264 and 14.x through 16.x before 16.0.0.296 on Windows and OS X and before 11.2.202.440 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-0313	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in February 2015, a different vulnerability than CVE-2015-0315, CVE-2015-0320, and CVE-2015-0322.
CVE-2015-0314	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0316, CVE-2015-0318, CVE-2015-0321, CVE-2015-0329, and CVE-2015-0330.
CVE-2015-0315	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0313, CVE-2015-0320, and CVE-2015-0322.

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

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

	of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0314, CVE-2015-0316, CVE-2015-0318, CVE-2015-0321, and CVE-2015-0329.
CVE-2015-0331	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0313, CVE-2015-0315, CVE-2015-0320, and CVE-2015-0322.
CVE-2015-0332	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0333, CVE-2015-0335, and CVE-2015-0339.
CVE-2015-0333	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0332, CVE-2015-0335, and CVE-2015-0339.
CVE-2015-0334	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-0336.
CVE-2015-0335	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0332, CVE-2015-0333, and CVE-2015-0339.
CVE-2015-0336	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-0334.
CVE-2015-0337	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows remote attackers to bypass the Same Origin Policy via unspecified vectors.

CVE-2015-0338	Integer overflow in Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-0339	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0332, CVE-2015-0333, and CVE-2015-0335.
CVE-2015-0340	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows remote attackers to bypass intended file-upload restrictions via unspecified vectors.
CVE-2015-0341	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0342.
CVE-2015-0342	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0341.
CVE-2015-0346	Double free vulnerability in Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0359.
CVE-2015-0347	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0350, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, CVE-2015-3042, and CVE-2015-3043.
CVE-2015-0348	Buffer overflow in Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code via unspecified vectors.

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

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

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

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

CVE-2015-1223	Multiple use-after-free vulnerabilities in core/html/HTMLInputElement.cpp in the DOM implementation in Blink, as used in Google Chrome before 41.0.2272.76, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger extraneous change events, as demonstrated by events for invalid input or input to read-only fields, related to the initializeTypeInParsing and updateType functions.
CVE-2015-1224	The VpxVideoDecoder::VpxDecode function in media/filters/vpx_video_decoder.cc in the vpxdecoder implementation in Google Chrome before 41.0.2272.76 does not ensure that alpha-plane dimensions are identical to image dimensions, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted VPx video data.
CVE-2015-1225	PDFium, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2015-1226	The DebuggerFunction::InitAgentHost function in browser/extensions/api/debugger/debugger_api.cc in Google Chrome before 41.0.2272.76 does not properly restrict what URLs are available as debugger targets, which allows remote attackers to bypass intended access restrictions via a crafted extension.
CVE-2015-1227	The DragImage::create function in platform/DragImage.cpp in Blink, as used in Google Chrome before 41.0.2272.76, does not initialize memory for image drawing, which allows remote attackers to have an unspecified impact by triggering a failed image decoding, as demonstrated by an image for which the default orientation cannot be used.
CVE-2015-1228	The RenderCounter::updateCounter function in core/rendering/RenderCounter.cpp in Blink, as used in Google Chrome before 41.0.2272.76, does not force a relayout operation and consequently does not initialize memory for a data structure, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted Cascading Style Sheets (CSS) token sequence.
CVE-2015-1229	net/http/proxy_client_socket.cc in Google Chrome before 41.0.2272.76 does not properly handle a 407 (aka Proxy Authentication Required) HTTP status code accompanied by a Set-Cookie header, which allows remote proxy servers to conduct cookie-injection attacks via a crafted response.
CVE-2015-1230	The getHiddenProperty function in bindings/core/v8/V8EventListenerList.h in Blink, as used in Google Chrome before 41.0.2272.76, has a name conflict with the AudioContext class, which allows remote

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

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

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

CVE-2015-1256	Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before 43.0.2357.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document that leverages improper handling of a shadow tree for a use element.
CVE-2015-1257	platform/graphics/filters/FEColorMatrix.cpp in the SVG implementation in Blink, as used in Google Chrome before 43.0.2357.65, does not properly handle an insufficient number of values in an feColorMatrix filter, which allows remote attackers to cause a denial of service (container overflow) or possibly have unspecified other impact via a crafted document.
CVE-2015-1258	Google Chrome before 43.0.2357.65 relies on libvpx code that was not built with an appropriate --size-limit value, which allows remote attackers to trigger a negative value for a size field, and consequently cause a denial of service or possibly have unspecified other impact, via a crafted frame size in VP9 video data.
CVE-2015-1259	PDFium, as used in Google Chrome before 43.0.2357.65, does not properly initialize memory, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2015-1260	Multiple use-after-free vulnerabilities in content/renderer/media/user_media_client_impl.cc in the WebRTC implementation in Google Chrome before 43.0.2357.65 allow remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that executes upon completion of a getUserMedia request.
CVE-2015-1262	platform/fonts/shaping/HarfBuzzShaper.cpp in Blink, as used in Google Chrome before 43.0.2357.65, does not initialize a certain width field, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted Unicode text.
CVE-2015-1263	The Spellcheck API implementation in Google Chrome before 43.0.2357.65 does not use an HTTPS session for downloading a Hunspell dictionary, which allows man-in-the-middle attackers to deliver incorrect spelling suggestions or possibly have unspecified other impact via a crafted file.
CVE-2015-1264	Cross-site scripting (XSS) vulnerability in Google Chrome before 43.0.2357.65 allows user-assisted remote attackers to inject arbitrary web script or HTML via crafted data that is improperly handled by the Bookmarks feature.
CVE-2015-1265	Multiple unspecified vulnerabilities in Google Chrome before 43.0.2357.65 allow attackers to cause a denial

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

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

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

	suggestions or possibly have unspecified other impact via a crafted file, a related issue to CVE-2015-1263.
CVE-2015-1289	Multiple unspecified vulnerabilities in Google Chrome before 44.0.2403.89 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1290	The Google V8 engine, as used in Google Chrome before 44.0.2403.89 and QtWebEngineCore in Qt before 5.5.1, allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via a crafted web site.
CVE-2015-1291	The ContainerNode::parserRemoveChild function in core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 45.0.2454.85, does not check whether a node is expected, which allows remote attackers to bypass the Same Origin Policy or cause a denial of service (DOM tree corruption) via a web site with crafted JavaScript code and IFRAME elements.
CVE-2015-1292	The NavigatorServiceWorker::serviceWorker function in modules/serviceworkers/NavigatorServiceWorker.cpp in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to bypass the Same Origin Policy by accessing a Service Worker.
CVE-2015-1293	The DOM implementation in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2015-1294	Use-after-free vulnerability in the SkMatrix::invertNonIdentity function in core/SkMatrix.cpp in Skia, as used in Google Chrome before 45.0.2454.85, allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering the use of matrix elements that lead to an infinite result during an inversion calculation.
CVE-2015-1295	Multiple use-after-free vulnerabilities in the PrintWebViewHelper class in components/printing/renderer/print_web_view_helper.cc in Google Chrome before 45.0.2454.85 allow user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact by triggering nested IPC messages during preparation for printing, as demonstrated by messages associated with PDF documents in conjunction with messages about printer capabilities.
CVE-2015-1296	The UnescapeURLWithAdjustmentsImpl implementation in net/base/escape.cc in Google Chrome before 45.0.2454.85 does not prevent display of Unicode LOCK characters in the omnibox, which makes it easier for remote attackers to spoof the SSL lock icon by placing one of these characters at the

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

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

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

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

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

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

	to bypass a CVE-2014-5333 protection mechanism via unspecified vectors.
CVE-2015-3098	Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allow remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-3099 and CVE-2015-3102.
CVE-2015-3099	Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allow remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-3098 and CVE-2015-3102.
CVE-2015-3100	Stack-based buffer overflow in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-3101	The Flash broker in Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe AIR SDK & Compiler before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, when Internet Explorer is used, allows attackers to perform a transition from Low Integrity to Medium Integrity via unspecified vectors.
CVE-2015-3102	Adobe Flash Player before 13.0.0.292 and 14.x through 18.x before 18.0.0.160 on Windows and OS X and before 11.2.202.466 on Linux, Adobe AIR before 18.0.0.144 on Windows and before 18.0.0.143 on OS X and Android, Adobe AIR SDK before 18.0.0.144 on Windows and before 18.0.0.143 on OS X, and Adobe

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

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

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

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

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

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

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

	enabled, allows remote attackers to read arbitrary files via unspecified vectors.
CVE-2015-3910	Multiple unspecified vulnerabilities in Google V8 before 4.3.61.21, as used in Google Chrome before 43.0.2357.65, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-4165	The snapshot API in Elasticsearch before 1.6.0 when another application exists on the system that can read Lucene files and execute code from them, is accessible by the attacker, and the Java VM on which Elasticsearch is running can write to a location that the other application can read and execute from, allows remote authenticated users to write to and create arbitrary snapshot metadata files, and potentially execute arbitrary code.
CVE-2015-4428	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4430, and CVE-2015-5117.
CVE-2015-4429	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2015-3126.
CVE-2015-4430	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, and CVE-2015-5117.
CVE-2015-4431	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and

	OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, and CVE-2015-3134.
CVE-2015-4432	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3135 and CVE-2015-5118.
CVE-2015-4433	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-3119, CVE-2015-3120, CVE-2015-3121, and CVE-2015-3122.
CVE-2015-5116	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2014-0578, CVE-2015-3115, CVE-2015-3116, and CVE-2015-3125.
CVE-2015-5117	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3118, CVE-2015-3124, CVE-2015-3127, CVE-2015-3128, CVE-2015-3129, CVE-2015-3131, CVE-2015-3132, CVE-2015-3136, CVE-2015-3137, CVE-2015-4428, and CVE-2015-4430.
CVE-2015-5118	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180,

	Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-3135 and CVE-2015-4432.
CVE-2015-5119	Use-after-free vulnerability in the ByteArray class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.296 and 14.x through 18.0.0.194 on Windows and OS X and 11.x through 11.2.202.468 on Linux allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content that overrides a valueOf function, as exploited in the wild in July 2015.
CVE-2015-5122	Use-after-free vulnerability in the DisplayObject class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.302 on Windows and OS X, 14.x through 18.0.0.203 on Windows and OS X, 11.x through 11.2.202.481 on Linux, and 12.x through 18.0.0.204 on Linux Chrome installations allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content that leverages improper handling of the opaqueBackground property, as exploited in the wild in July 2015.
CVE-2015-5123	Use-after-free vulnerability in the BitmapData class in the ActionScript 3 (AS3) implementation in Adobe Flash Player 13.x through 13.0.0.302 on Windows and OS X, 14.x through 18.0.0.203 on Windows and OS X, 11.x through 11.2.202.481 on Linux, and 12.x through 18.0.0.204 on Linux Chrome installations allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content that overrides a valueOf function, as exploited in the wild in July 2015.
CVE-2015-5124	Adobe Flash Player before 13.0.0.302 and 14.x through 18.x before 18.0.0.203 on Windows and OS X and before 11.2.202.481 on Linux, Adobe AIR before 18.0.0.180, Adobe AIR SDK before 18.0.0.180, and Adobe AIR SDK & Compiler before 18.0.0.180 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-3117, CVE-2015-3123, CVE-2015-3130, CVE-2015-3133, CVE-2015-3134, and CVE-2015-4431.
CVE-2015-5125	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to cause a denial of service (vector-

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

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

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

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

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

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

	allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5564	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, and CVE-2015-5565.
CVE-2015-5565	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, and CVE-2015-5564.
CVE-2015-5566	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5567	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5579.

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

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

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

	11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, and CVE-2015-6677.
CVE-2015-5605	The regular-expression implementation in Google V8, as used in Google Chrome before 44.0.2403.89, mishandles interrupts, which allows remote attackers to cause a denial of service (application crash) via crafted JavaScript code, as demonstrated by an error in garbage collection during allocation of a stack-overflow exception message.
CVE-2015-5700	mktexlsr revision 22855 through revision 36625 as packaged in texlive allows local users to write to arbitrary files via a symlink attack.
CVE-2015-6580	Multiple unspecified vulnerabilities in Google V8 before 4.5.103.29, as used in Google Chrome before 45.0.2454.85, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-6581	Double free vulnerability in the opj_j2k_copy_default_tcp_and_create_tcd function in j2k.c in OpenJPEG before r3002, as used in PDFium in Google Chrome before 45.0.2454.85, allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by triggering a memory-allocation failure.
CVE-2015-6582	The decompose function in platform/transforms/TransformationMatrix.cpp in Blink, as used in Google Chrome before 45.0.2454.85, does not verify that a matrix inversion succeeded, which allows remote attackers to cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified other impact via a crafted web site.
CVE-2015-6583	Google Chrome before 45.0.2454.85 does not display a location bar for a hosted app's window after navigation away from the installation site, which might make it easier for remote attackers to spoof content via a crafted app, related to browser.cc and hosted_app_browser_controller.cc.
CVE-2015-6676	Buffer overflow in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code

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

CVE-2015-6757	Use-after-free vulnerability in content/browser/service_worker/embedded_worker_instance.cc in the ServiceWorker implementation in Google Chrome before 46.0.2490.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging object destruction in a callback.
CVE-2015-6758	The CPDF_Document::GetPage function in fpdfapi/fpdf_parser/fpdf_parser_document.cpp in PDFium, as used in Google Chrome before 46.0.2490.71, does not properly perform a cast of a dictionary object, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.
CVE-2015-6759	The shouldTreatAsUniqueOrigin function in platform/weborigin/SecurityOrigin.cpp in Blink, as used in Google Chrome before 46.0.2490.71, does not ensure that the origin of a LocalStorage resource is considered unique, which allows remote attackers to obtain sensitive information via vectors involving a blob: URL.
CVE-2015-6760	The Image11::map function in renderer/d3d/d3d11/Image11.cpp in libANGLE, as used in Google Chrome before 46.0.2490.71, mishandles mapping failures after device-lost events, which allows remote attackers to cause a denial of service (invalid read or write) or possibly have unspecified other impact via vectors involving a removed device.
CVE-2015-6761	The update_dimensions function in libavcodec/vp8.c in FFmpeg through 2.8.1, as used in Google Chrome before 46.0.2490.71 and other products, relies on a coefficient-partition count during multi-threaded operation, which allows remote attackers to cause a denial of service (race condition and memory corruption) or possibly have unspecified other impact via a crafted WebM file.
CVE-2015-6762	The CSSFontFaceSrcValue::fetch function in core/css/CSSFontFaceSrcValue.cpp in the Cascading Style Sheets (CSS) implementation in Blink, as used in Google Chrome before 46.0.2490.71, does not use the CORS cross-origin request algorithm when a font's URL appears to be a same-origin URL, which allows remote web servers to bypass the Same Origin Policy via a redirect.
CVE-2015-6763	Multiple unspecified vulnerabilities in Google Chrome before 46.0.2490.71 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-6764	The BasicJsonStringifier::SerializeJSArray function in json-stringifier.h in the JSON stringifier in Google V8, as used in Google Chrome before 47.0.2526.73, improperly loads array elements, which allows remote

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

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

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

CVE-2015-6790	The WebPageSerializerImpl::openTagToString function in WebKit/Source/web/WebPageSerializerImpl.cpp in the page serializer in Google Chrome before 47.0.2526.80 does not properly use HTML entities, which might allow remote attackers to inject arbitrary web script or HTML via a crafted document, as demonstrated by a double-quote character inside a single-quoted string.
CVE-2015-6791	Multiple unspecified vulnerabilities in Google Chrome before 47.0.2526.80 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-6792	The MIDI subsystem in Google Chrome before 47.0.2526.106 does not properly handle the sending of data, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors, related to midi_manager.cc, midi_manager_alsa.cc, and midi_manager_mac.cc, a different vulnerability than CVE-2015-8664.
CVE-2015-7625	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7626, CVE-2015-7627, CVE-2015-7630, CVE-2015-7633, and CVE-2015-7634.
CVE-2015-7626	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7627, CVE-2015-7630, CVE-2015-7633, and CVE-2015-7634.
CVE-2015-7627	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7626, CVE-2015-7630, CVE-2015-7633, and CVE-2015-7634.
CVE-2015-7628	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before

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

CVE-2015-7634	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7630, and CVE-2015-7633.
CVE-2015-7635	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7636	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7637	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7638	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

	CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8407	Stack-based buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8457.
CVE-2015-8408	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8409	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2015-8440 and CVE-2015-8453.
CVE-2015-8410	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8411,

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

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

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

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

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

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

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

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

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

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

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

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

	CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8438	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted XML object that is mishandled during a toString call, a different vulnerability than CVE-2015-8446.
CVE-2015-8439	The SharedObject object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code by leveraging an unspecified "type confusion" during a getRemote call, a different vulnerability than CVE-2015-8456.
CVE-2015-8440	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2015-8409 and CVE-2015-8453.
CVE-2015-8441	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059,

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

	CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8444	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8445	Integer overflow in the Shader filter implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a large BitmapData source object.
CVE-2015-8446	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via an MP3 file with COMM tags that are mishandled during memory allocation, a different vulnerability than CVE-2015-8438.
CVE-2015-8447	Use-after-free vulnerability in the Color object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted setTransform arguments, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424,

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

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

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

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

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

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

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

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

	CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, and CVE-2015-8649.
CVE-2015-8651	Integer overflow in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-8652	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, CVE-2015-8455, CVE-2015-8654, CVE-2015-8656, CVE-2015-8657, CVE-2015-8658, and CVE-2015-8820.
CVE-2015-8653	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted MPEG-4 data, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, CVE-2015-8454, CVE-2015-8655, CVE-2015-8821, and CVE-2015-8822.

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

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

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

	CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, CVE-2015-8454, CVE-2015-8653, CVE-2015-8655, and CVE-2015-8821.
CVE-2015-8823	Use-after-free vulnerability in the TextField object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted text property, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, CVE-2015-8454, CVE-2015-8653, CVE-2015-8655, CVE-2015-8821, and CVE-2015-8822.
CVE-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-2015-9253	An issue was discovered in PHP 7.3.x before 7.3.0alpha3, 7.2.x before 7.2.8, and before 7.1.20. The php-fpm master process restarts a child process in an endless loop when using program execution functions (e.g., passthru, exec, shell_exec, or system) with a non-blocking STDIN stream, causing this master process to consume 100% of the CPU, and consume disk space with a large volume of error logs, as demonstrated by an attack by a customer of a shared-hosting facility.

CVE-2016-0959	Use after free vulnerability in Adobe Flash Player Desktop Runtime before 20.0.0.267, Adobe Flash Player Extended Support Release before 18.0.0.324, Adobe Flash Player for Google Chrome before 20.0.0.267, Adobe Flash Player for Microsoft Edge and Internet Explorer 11 before 20.0.0.267, Adobe Flash Player for Internet Explorer 10 and 11 before 20.0.0.267, Adobe Flash Player for Linux before 11.2.202.559, AIR Desktop Runtime before 20.0.0.233, AIR SDK before 20.0.0.233, AIR SDK & Compiler before 20.0.0.233, AIR for Android before 20.0.0.233.
CVE-2016-0960	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.
CVE-2016-0961	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.
CVE-2016-0962	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.
CVE-2016-0963	Integer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code

	via unspecified vectors, a different vulnerability than CVE-2016-0993 and CVE-2016-1010.
CVE-2016-0964	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.
CVE-2016-0965	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.
CVE-2016-0966	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.
CVE-2016-0967	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977,

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

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

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

	CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, and CVE-2016-0981.
CVE-2016-0981	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, and CVE-2016-0980.
CVE-2016-0982	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0973, CVE-2016-0974, CVE-2016-0975, CVE-2016-0983, and CVE-2016-0984.
CVE-2016-0983	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0973, CVE-2016-0974, CVE-2016-0975, CVE-2016-0982, and CVE-2016-0984.
CVE-2016-0984	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0973, CVE-2016-0974, CVE-2016-0975, CVE-2016-0982, and CVE-2016-0983.
CVE-2016-0985	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow

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

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

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

CVE-2016-0999	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, and CVE-2016-1000.
CVE-2016-1000	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, and CVE-2016-0999.
CVE-2016-1001	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2016-1002	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, and CVE-2016-1005.
CVE-2016-1005	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (uninitialized pointer dereference and memory corruption) via crafted MPEG-4 data, a different vulnerability than CVE-2016-0960, CVE-2016-0961,

	CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, and CVE-2016-1002.
CVE-2016-1006	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to bypass the ASLR protection mechanism via JIT data.
CVE-2016-10087	The png_set_text_2 function in libpng 0.71 before 1.0.67, 1.2.x before 1.2.57, 1.4.x before 1.4.20, 1.5.x before 1.5.28, and 1.6.x before 1.6.27 allows context-dependent attackers to cause a NULL pointer dereference vectors involving loading a text chunk into a png structure, removing the text, and then adding another text chunk to the structure.
CVE-2016-1010	Integer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0963 and CVE-2016-0993.
CVE-2016-1011	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1013, CVE-2016-1016, CVE-2016-1017, and CVE-2016-1031.
CVE-2016-1012	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1013	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1011, CVE-2016-1016, CVE-2016-1017, and CVE-2016-1031.
CVE-2016-1014	Untrusted search path vulnerability in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows local users to gain

	privileges via a Trojan horse resource in an unspecified directory.
CVE-2016-1015	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code by overriding NetConnection object properties to leverage an unspecified "type confusion," a different vulnerability than CVE-2016-1019.
CVE-2016-1016	Use-after-free vulnerability in the Transform object implementation in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via a flash.geom.Matrix callback, a different vulnerability than CVE-2016-1011, CVE-2016-1013, CVE-2016-1017, and CVE-2016-1031.
CVE-2016-10165	The Type_MLU_Read function in cmstypes.c in Little CMS (aka lcms2) allows remote attackers to obtain sensitive information or cause a denial of service via an image with a crafted ICC profile, which triggers an out-of-bounds heap read.
CVE-2016-1017	Use-after-free vulnerability in the LoadVars.decode function in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1011, CVE-2016-1013, CVE-2016-1016, and CVE-2016-1031.
CVE-2016-1018	Stack-based buffer overflow in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via crafted JPEG-XR data.
CVE-2016-1019	Adobe Flash Player 21.0.0.197 and earlier allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unspecified vectors, as exploited in the wild in April 2016.
CVE-2016-1020	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.

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

CVE-2016-1026	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1027	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1028	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1029	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1030	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to bypass intended access restrictions via unspecified vectors.
CVE-2016-1031	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different

	vulnerability than CVE-2016-1011, CVE-2016-1013, CVE-2016-1016, and CVE-2016-1017.
CVE-2016-10317	The fill_threshhold_buffer function in base/gxht_thresh.c in Artifex Software, Inc. Ghostscript 9.20 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 PostScript document.
CVE-2016-1032	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, and CVE-2016-1033.
CVE-2016-1033	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, and CVE-2016-1032.
CVE-2016-1096	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1097	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1098	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1099	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack

	vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1100	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1101	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1102	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1103	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1104	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1105	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1106	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1107	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.

CVE-2016-1108	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1109	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1110	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-1612	The LoadIC::UpdateCaches function in ic/ic.cc in Google V8, as used in Google Chrome before 48.0.2564.82, does not ensure receiver compatibility before performing a cast of an unspecified variable, which allows remote attackers to cause a denial of service or possibly have unknown other impact via crafted JavaScript code.
CVE-2016-1613	Multiple use-after-free vulnerabilities in the formfiller implementation in PDFium, as used in Google Chrome before 48.0.2564.82, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document, related to improper tracking of the destruction of (1) IPWL_FocusHandler and (2) IPWL_Provider objects.
CVE-2016-1614	The UnacceleratedImageBufferSurface class in WebKit/Source/platform/graphics/UnacceleratedImageBufferSurface.cpp in Blink, as used in Google Chrome before 48.0.2564.82, mishandles the initialization mode, which allows remote attackers to obtain sensitive information from process memory via a crafted web site.
CVE-2016-1615	The Omnibox implementation in Google Chrome before 48.0.2564.82 allows remote attackers to spoof a document's origin via unspecified vectors.
CVE-2016-1616	The CustomButton::AcceleratorPressed function in ui/views/controls/button/custom_button.cc in Google Chrome before 48.0.2564.82 allows remote attackers to spoof URLs via vectors involving an unfocused custom button.
CVE-2016-1617	The CSPSource::schemeMatches function in WebKit/Source/core/frame/csp/CSPSource.cpp in the Content Security Policy (CSP) implementation in Blink, as used

	in Google Chrome before 48.0.2564.82, does not apply http policies to https URLs and does not apply ws policies to wss URLs, which makes it easier for remote attackers to determine whether a specific HSTS web site has been visited by reading a CSP report.
CVE-2016-1618	Blink, as used in Google Chrome before 48.0.2564.82, does not ensure that a proper cryptographicallyRandomValues random number generator is used, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors.
CVE-2016-1619	Multiple integer overflows in the (1) sycc422_to_rgb and (2) sycc444_to_rgb functions in fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 48.0.2564.82, allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted PDF document.
CVE-2016-1620	Multiple unspecified vulnerabilities in Google Chrome before 48.0.2564.82 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1622	The Extensions subsystem in Google Chrome before 48.0.2564.109 does not prevent use of the Object.defineProperty method to override intended extension behavior, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.
CVE-2016-1623	The DOM implementation in Google Chrome before 48.0.2564.109 does not properly restrict frame-attach operations from occurring during or after frame-detach operations, which allows remote attackers to bypass the Same Origin Policy via a crafted web site, related to FrameLoader.cpp, HTMLFrameOwnerElement.h, LocalFrame.cpp, and WebLocalFrameImpl.cpp.
CVE-2016-1624	Integer underflow in the ProcessCommandsInternal function in dec/decode.c in Brotli, as used in Google Chrome before 48.0.2564.109, allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted data with brotli compression.
CVE-2016-1625	The Chrome Instant feature in Google Chrome before 48.0.2564.109 does not ensure that a New Tab Page (NTP) navigation target is on the most-visited or suggestions list, which allows remote attackers to bypass intended restrictions via unspecified vectors, related to instant_service.cc and search_tab_helper.cc.
CVE-2016-1626	The opj_pi_update_decode_poc function in pi.c in OpenJPEG, as used in PDFium in Google Chrome before 48.0.2564.109, miscalculates a certain layer

	index value, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document.
CVE-2016-1627	The Developer Tools (aka DevTools) subsystem in Google Chrome before 48.0.2564.109 does not validate URL schemes and ensure that the remoteBase parameter is associated with a chrome-devtools-frontend.appspot.com URL, which allows remote attackers to bypass intended access restrictions via a crafted URL, related to browser/devtools/devtools_ui_bindings.cc and WebKit/Source/devtools/front_end/Runtime.js.
CVE-2016-1628	pi.c in OpenJPEG, as used in PDFium in Google Chrome before 48.0.2564.109, does not validate a certain precision value, which allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via a crafted JPEG 2000 image in a PDF document, related to the opj_pi_next_rpcl, opj_pi_next_pcrl, and opj_pi_next_cprl functions.
CVE-2016-1629	Google Chrome before 48.0.2564.116 allows remote attackers to bypass the Blink Same Origin Policy and a sandbox protection mechanism via unspecified vectors.
CVE-2016-1630	The ContainerNode::parserRemoveChild function in WebKit/Source/core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 49.0.2623.75, mishandles widget updates, which makes it easier for remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1631	The PPB_Flash_MessageLoop_Impl::InternalRun function in content/renderer/pepper/ppb_flash_message_loop_impl.cc in the Pepper plugin in Google Chrome before 49.0.2623.75 mishandles nested message loops, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1632	The Extensions subsystem in Google Chrome before 49.0.2623.75 does not properly maintain own properties, which allows remote attackers to bypass intended access restrictions via crafted JavaScript code that triggers an incorrect cast, related to extensions/renderer/v8_helpers.h and gin/converter.h.
CVE-2016-1633	Use-after-free vulnerability in Blink, as used in Google Chrome before 49.0.2623.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2016-1634	Use-after-free vulnerability in the StyleResolver::appendCSSStyleSheet function in WebKit/Source/core/css/resolver/StyleResolver.cpp in Blink, as used in Google Chrome before 49.0.2623.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted

	web site that triggers Cascading Style Sheets (CSS) style invalidation during a certain subtree-removal action.
CVE-2016-1635	extensions/renderer/render_frame_observer_natives.cc in Google Chrome before 49.0.2623.75 does not properly consider object lifetimes and re-entrancy issues during OnDocumentElementCreated handling, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors.
CVE-2016-1636	The PendingScript::notifyFinished function in WebKit/Source/core/dom/PendingScript.cpp in Google Chrome before 49.0.2623.75 relies on memory-cache information about integrity-check occurrences instead of integrity-check successes, which allows remote attackers to bypass the Subresource Integrity (aka SRI) protection mechanism by triggering two loads of the same resource.
CVE-2016-1637	The SkATan2_255 function in effects/gradients/SkSweepGradient.cpp in Skia, as used in Google Chrome before 49.0.2623.75, mishandles arctangent calculations, which allows remote attackers to obtain sensitive information via a crafted web site.
CVE-2016-1638	extensions/renderer/resources/platform_app.js in the Extensions subsystem in Google Chrome before 49.0.2623.75 does not properly restrict use of Web APIs, which allows remote attackers to bypass intended access restrictions via a crafted platform app.
CVE-2016-1639	Use-after-free vulnerability in browser/extensions/api/webrtc_audio_private/webrtc_audio_private_api.cc in the WebRTC Audio Private API implementation in Google Chrome before 49.0.2623.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect reliance on the resource context pointer.
CVE-2016-1640	The Web Store inline-installer implementation in the Extensions UI in Google Chrome before 49.0.2623.75 does not block installations upon deletion of an installation frame, which makes it easier for remote attackers to trick a user into believing that an installation request originated from the user's next navigation target via a crafted web site.
CVE-2016-1641	Use-after-free vulnerability in content/browser/web_contents/web_contents_impl.cc in Google Chrome before 49.0.2623.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering an image download after a certain data structure is deleted, as demonstrated by a favicon.ico download.

CVE-2016-1642	Multiple unspecified vulnerabilities in Google Chrome before 49.0.2623.75 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1643	The ImageInputType::ensurePrimaryContent function in WebKit/Source/core/html/forms/ImageInputType.cpp in Blink, as used in Google Chrome before 49.0.2623.87, does not properly maintain the user agent shadow DOM, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2016-1644	WebKit/Source/core/layout/LayoutObject.cpp in Blink, as used in Google Chrome before 49.0.2623.87, does not properly restrict relayout scheduling, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted HTML document.
CVE-2016-1645	Multiple integer signedness errors in the opj_j2k_update_image_data function in j2k.c in OpenJPEG, as used in PDFium in Google Chrome before 49.0.2623.87, allow remote attackers to cause a denial of service (incorrect cast and out-of-bounds write) or possibly have unspecified other impact via crafted JPEG 2000 data.
CVE-2016-1646	The Array.prototype.concat implementation in builtins.cc in Google V8, as used in Google Chrome before 49.0.2623.108, does not properly consider element data types, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-1647	Use-after-free vulnerability in the RenderWidgetHostImpl::Destroy function in content/browser/renderer_host/render_widget_host_impl.cc in the Navigation implementation in Google Chrome before 49.0.2623.108 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2016-1648	Use-after-free vulnerability in the GetLoadTimes function in renderer/loadtimes_extension_bindings.cc in the Extensions implementation in Google Chrome before 49.0.2623.108 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-1649	The Program::getUniformInternal function in Program.cpp in libANGLE, as used in Google Chrome before 49.0.2623.108, does not properly handle a certain data-type mismatch, which allows remote attackers to cause a denial of service (buffer overflow)

	or possibly have unspecified other impact via crafted shader stages.
CVE-2016-1650	The PageCaptureSaveAsMHTMLFunction::ReturnFailure function in browser/extensions/api/page_capture/page_capture_api.cc in Google Chrome before 49.0.2623.108 allows attackers to cause a denial of service or possibly have unspecified other impact by triggering an error in creating an MHTML document.
CVE-2016-1651	fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 50.0.2661.75, does not properly implement the sycc420_to_rgb and sycc422_to_rgb functions, which allows remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via crafted JPEG 2000 data in a PDF document.
CVE-2016-1652	Cross-site scripting (XSS) vulnerability in the ModuleSystem::RequireForJsInner function in extensions/renderer/module_system.cc in the Extensions subsystem in Google Chrome before 50.0.2661.75 allows remote attackers to inject arbitrary web script or HTML via a crafted web site, aka "Universal XSS (UXSS)."
CVE-2016-1653	The LoadBuffer implementation in Google V8, as used in Google Chrome before 50.0.2661.75, mishandles data types, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers an out-of-bounds write operation, related to compiler/pipeline.cc and compiler/simplified-lowering.cc.
CVE-2016-1654	The media subsystem in Google Chrome before 50.0.2661.75 does not initialize an unspecified data structure, which allows remote attackers to cause a denial of service (invalid read operation) via unknown vectors.
CVE-2016-1655	Google Chrome before 50.0.2661.75 does not properly consider that frame removal may occur during callback execution, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted extension.
CVE-2016-1657	The WebContentsImpl::FocusLocationBarByDefault function in content/browser/web_contents/web_contents_impl.cc in Google Chrome before 50.0.2661.75 mishandles focus for certain about:blank pages, which allows remote attackers to spoof the address bar via a crafted URL.
CVE-2016-1658	The Extensions subsystem in Google Chrome before 50.0.2661.75 incorrectly relies on GetOrigin method calls for origin comparisons, which allows remote

	attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted extension.
CVE-2016-1659	Multiple unspecified vulnerabilities in Google Chrome before 50.0.2661.75 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1660	Blink, as used in Google Chrome before 50.0.2661.94, mishandles assertions in the WTF::BitArray and WTF::double_conversion::Vector classes, which allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via a crafted web site.
CVE-2016-1661	Blink, as used in Google Chrome before 50.0.2661.94, does not ensure that frames satisfy a check for the same renderer process in addition to a Same Origin Policy check, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted web site, related to BindingSecurity.cpp and DOMWindow.cpp.
CVE-2016-1662	extensions/renderer/gc_callback.cc in Google Chrome before 50.0.2661.94 does not prevent fallback execution once the Garbage Collection callback has started, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors.
CVE-2016-1663	The SerializedScriptValue::transferArrayBuffers function in WebKit/Source/bindings/core/v8/SerializedScriptValue.cpp in the V8 bindings in Blink, as used in Google Chrome before 50.0.2661.94, mishandles certain array-buffer data structures, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site.
CVE-2016-1664	The HistoryController::UpdateForCommit function in content/renderer/history_controller.cc in Google Chrome before 50.0.2661.94 mishandles the interaction between subframe forward navigations and other forward navigations, which allows remote attackers to spoof the address bar via a crafted web site.
CVE-2016-1665	The JSGenericLowering class in compiler/js-generic-lowering.cc in Google V8, as used in Google Chrome before 50.0.2661.94, mishandles comparison operators, which allows remote attackers to obtain sensitive information via crafted JavaScript code.
CVE-2016-1666	Multiple unspecified vulnerabilities in Google Chrome before 50.0.2661.94 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1667	The TreeScope::adoptIfNeeded function in WebKit/Source/core/dom/TreeScope.cpp in the DOM

	implementation in Blink, as used in Google Chrome before 50.0.2661.102, does not prevent script execution during node-adoption operations, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1668	The forEachForBinding function in WebKit/Source/bindings/core/v8/Iterable.h in the V8 bindings in Blink, as used in Google Chrome before 50.0.2661.102, uses an improper creation context, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1669	The Zone::New function in zone.cc in Google V8 before 5.0.71.47, as used in Google Chrome before 50.0.2661.102, does not properly determine when to expand certain memory allocations, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-1670	Race condition in the ResourceDispatcherHostImpl::BeginRequest function in content/browser/loader/resource_dispatcher_host_impl.cc in Google Chrome before 50.0.2661.102 allows remote attackers to make arbitrary HTTP requests by leveraging access to a renderer process and reusing a request ID.
CVE-2016-1672	The ModuleSystem::RequireForJsInner function in extensions/renderer/module_system.cc in the extension bindings in Google Chrome before 51.0.2704.63 mishandles properties, which allows remote attackers to conduct bindings-interception attacks and bypass the Same Origin Policy via unspecified vectors.
CVE-2016-1673	Blink, as used in Google Chrome before 51.0.2704.63, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2016-1674	The extensions subsystem in Google Chrome before 51.0.2704.63 allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2016-1675	Blink, as used in Google Chrome before 51.0.2704.63, allows remote attackers to bypass the Same Origin Policy by leveraging the mishandling of Document reattachment during destruction, related to FrameLoader.cpp and LocalFrame.cpp.
CVE-2016-1676	extensions/renderer/resources/binding.js in the extension bindings in Google Chrome before 51.0.2704.63 does not properly use prototypes, which allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2016-1677	uri.js in Google V8 before 5.1.281.26, as used in Google Chrome before 51.0.2704.63, uses an incorrect array type, which allows remote attackers to obtain

	sensitive information by calling the decodeURI function and leveraging "type confusion."
CVE-2016-1678	objects.cc in Google V8 before 5.0.71.32, as used in Google Chrome before 51.0.2704.63, does not properly restrict lazy deoptimization, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-1679	The ToV8Value function in content/child/v8_value_converter_impl.cc in the V8 bindings in Google Chrome before 51.0.2704.63 does not properly restrict use of getters and setters, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-1680	Use-after-free vulnerability in ports/SkFontHost_FreeType.cpp in Skia, as used in Google Chrome before 51.0.2704.63, allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2016-1681	Heap-based buffer overflow in the opj_j2k_read_SPCod_SPCoc function in j2k.c in OpenJPEG, as used in PDFium in Google Chrome before 51.0.2704.63, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.
CVE-2016-1682	The ServiceWorkerContainer::registerServiceWorkerImpl function in WebKit/Source/modules/serviceworkers/ServiceWorkerContainer.cpp in Blink, as used in Google Chrome before 51.0.2704.63, allows remote attackers to bypass the Content Security Policy (CSP) protection mechanism via a ServiceWorker registration.
CVE-2016-1683	numbers.c in libxslt before 1.1.29, as used in Google Chrome before 51.0.2704.63, mishandles namespace nodes, which allows remote attackers to cause a denial of service (out-of-bounds heap memory access) or possibly have unspecified other impact via a crafted document.
CVE-2016-1684	numbers.c in libxslt before 1.1.29, as used in Google Chrome before 51.0.2704.63, mishandles the i format token for xsl:number data, which allows remote attackers to cause a denial of service (integer overflow or resource consumption) or possibly have unspecified other impact via a crafted document.
CVE-2016-1685	core/fxge/ge/fx_ge_text.cpp in PDFium, as used in Google Chrome before 51.0.2704.63, miscalculates certain index values, which allows remote attackers to

	cause a denial of service (out-of-bounds read) via a crafted PDF document.
CVE-2016-1686	The CPDF_DIBSource::CreateDecoder function in core/fpdfapi/fpdf_render/fpdf_render_loadimage.cpp in PDFium, as used in Google Chrome before 51.0.2704.63, mishandles decoder-initialization failure, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document.
CVE-2016-1687	The renderer implementation in Google Chrome before 51.0.2704.63 does not properly restrict public exposure of classes, which allows remote attackers to obtain sensitive information via vectors related to extensions.
CVE-2016-1688	The regexp (aka regular expression) implementation in Google V8 before 5.0.71.40, as used in Google Chrome before 51.0.2704.63, mishandles external string sizes, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted JavaScript code.
CVE-2016-1689	Heap-based buffer overflow in content/renderer/media/canvas_capture_handler.cc in Google Chrome before 51.0.2704.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site.
CVE-2016-1690	The Autofill implementation in Google Chrome before 51.0.2704.63 mishandles the interaction between field updates and JavaScript code that triggers a frame deletion, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site, a different vulnerability than CVE-2016-1701.
CVE-2016-1691	Skia, as used in Google Chrome before 51.0.2704.63, mishandles coincidence runs, which allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted curves, related to SkOpCoincidence.cpp and SkPathOpsCommon.cpp.
CVE-2016-1692	WebKit/Source/core/css/StyleSheetContents.cpp in Blink, as used in Google Chrome before 51.0.2704.63, permits cross-origin loading of CSS stylesheets by a ServiceWorker even when the stylesheet download has an incorrect MIME type, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1693	browser/safe_browsing/srt_field_trial_win.cc in Google Chrome before 51.0.2704.63 does not use the HTTPS service on dl.google.com to obtain the Software Removal Tool, which allows remote attackers to spoof the chrome_cleanup_tool.exe (aka CCT) file via a man-in-the-middle attack on an HTTP session.

CVE-2016-1694	browser/browsing_data/browsing_data_remover.cc in Google Chrome before 51.0.2704.63 deletes HPKP pins during cache clearing, which makes it easier for remote attackers to spoof web sites via a valid certificate from an arbitrary recognized Certification Authority.
CVE-2016-1695	Multiple unspecified vulnerabilities in Google Chrome before 51.0.2704.63 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1696	The extensions subsystem in Google Chrome before 51.0.2704.79 does not properly restrict bindings access, which allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2016-1697	The FrameLoader::startLoad function in WebKit/Source/core/loader/FrameLoader.cpp in Blink, as used in Google Chrome before 51.0.2704.79, does not prevent frame navigations during DocumentLoader detach operations, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.
CVE-2016-1698	The createCustomType function in extensions/renderer/resources/binding.js in the extension bindings in Google Chrome before 51.0.2704.79 does not validate module types, which might allow attackers to load arbitrary modules or obtain sensitive information by leveraging a poisoned definition.
CVE-2016-1699	WebKit/Source/devtools/front_end/devtools.js in the Developer Tools (aka DevTools) subsystem in Blink, as used in Google Chrome before 51.0.2704.79, does not ensure that the remoteFrontendUrl parameter is associated with a chrome-devtools-frontend.appspot.com URL, which allows remote attackers to bypass intended access restrictions via a crafted URL.
CVE-2016-1700	extensions/renderer/runtime_custom_bindings.cc in Google Chrome before 51.0.2704.79 does not consider side effects during creation of an array of extension views, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to extensions.
CVE-2016-1701	The Autofill implementation in Google Chrome before 51.0.2704.79 mishandles the interaction between field updates and JavaScript code that triggers a frame deletion, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site, a different vulnerability than CVE-2016-1690.
CVE-2016-1702	The SkRegion::readFromMemory function in core/SkRegion.cpp in Skia, as used in Google Chrome before 51.0.2704.79, does not validate the interval

	count, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted serialized data.
CVE-2016-1703	Multiple unspecified vulnerabilities in Google Chrome before 51.0.2704.79 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1704	Multiple unspecified vulnerabilities in Google Chrome before 51.0.2704.103 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1705	Multiple unspecified vulnerabilities in Google Chrome before 52.0.2743.82 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1706	The PPAPI implementation in Google Chrome before 52.0.2743.82 does not validate the origin of IPC messages to the plugin broker process that should have come from the browser process, which allows remote attackers to bypass a sandbox protection mechanism via an unexpected message type, related to broker_process_dispatcher.cc, ppapi_plugin_process_host.cc, ppapi_thread.cc, and render_frame_message_filter.cc.
CVE-2016-1707	ios/web/web_state/ui/crw_web_controller.mm in Google Chrome before 52.0.2743.82 on iOS does not ensure that an invalid URL is replaced with the about:blank URL, which allows remote attackers to spoof the URL display via a crafted web site.
CVE-2016-1708	The Chrome Web Store inline-installation implementation in the Extensions subsystem in Google Chrome before 52.0.2743.82 does not properly consider object lifetimes during progress observation, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site.
CVE-2016-1709	Heap-based buffer overflow in the ByteArray::Get method in data/byte_array.cc in Google sfntly before 2016-06-10, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted SFNT font.
CVE-2016-1710	The ChromeClientImpl::createWindow method in WebKit/Source/web/ChromeClientImpl.cpp in Blink, as used in Google Chrome before 52.0.2743.82, does not prevent window creation by a deferred frame, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1711	WebKit/Source/core/loader/FrameLoader.cpp in Blink, as used in Google Chrome before 52.0.2743.82, does

	not disable frame navigation during a detach operation on a DocumentLoader object, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-2051	Multiple unspecified vulnerabilities in Google V8 before 4.8.271.17, as used in Google Chrome before 48.0.2564.82, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-2052	Multiple unspecified vulnerabilities in HarfBuzz before 1.0.6, as used in Google Chrome before 48.0.2564.82, allow attackers to cause a denial of service or possibly have other impact via crafted data, as demonstrated by a buffer over-read resulting from an inverted length check in hb-ot-font.cc, a different issue than CVE-2015-8947.
CVE-2016-2843	Multiple unspecified vulnerabilities in Google V8 before 4.9.385.26, as used in Google Chrome before 49.0.2623.75, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-2844	WebKit/Source/core/layout/LayoutBlock.cpp in Blink, as used in Google Chrome before 49.0.2623.75, does not properly determine when anonymous block wrappers may exist, which allows remote attackers to cause a denial of service (incorrect cast and assertion failure) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-2845	The Content Security Policy (CSP) implementation in Blink, as used in Google Chrome before 49.0.2623.75, does not ignore a URL's path component in the case of a ServiceWorker fetch, which allows remote attackers to obtain sensitive information about visited web pages by reading CSP violation reports, related to FrameFetchContext.cpp and ResourceFetcher.cpp.
CVE-2016-3508	Unspecified vulnerability in Oracle Java SE 6u115, 7u101, and 8u92; Java SE Embedded 8u91; and JRockit R28.3.10 allows remote attackers to affect availability via vectors related to JAXP, a different vulnerability than CVE-2016-3500.
CVE-2016-3550	Unspecified vulnerability in Oracle Java SE 6u115, 7u101, and 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality via vectors related to Hotspot.
CVE-2016-3587	Unspecified vulnerability in Oracle Java SE 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot.
CVE-2016-3598	Unspecified vulnerability in Oracle Java SE 8u92 and Java SE Embedded 8u91 allows remote attackers

	to affect confidentiality, integrity, and availability via vectors related to Libraries, a different vulnerability than CVE-2016-3610.
CVE-2016-3606	Unspecified vulnerability in Oracle Java SE 7u101 and 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot.
CVE-2016-3610	Unspecified vulnerability in Oracle Java SE 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Libraries, a different vulnerability than CVE-2016-3598.
CVE-2016-3616	The cjpeg utility in libjpeg allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or execute arbitrary code via a crafted file.
CVE-2016-3679	Multiple unspecified vulnerabilities in Google V8 before 4.9.385.33, as used in Google Chrome before 49.0.2623.108, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-4108	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4109	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4110	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4111	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4112	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack

	vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4113	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4114	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4115	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4116	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4117	Adobe Flash Player 21.0.0.226 and earlier allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in May 2016.
CVE-2016-4120	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4160, CVE-2016-4161, CVE-2016-4162, and CVE-2016-4163.
CVE-2016-4121	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1097, CVE-2016-1106, CVE-2016-1107, CVE-2016-1108, CVE-2016-1109, CVE-2016-1110, CVE-2016-4108, and CVE-2016-4110.

CVE-2016-4122	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4123	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4124	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4125	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4127	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4128	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4129	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4130	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4131	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash

	libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4132	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4133	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4134	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4135	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4136	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4137	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4138	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4139	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack

	vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4140	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4141	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4142	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4143	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4144	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4145	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4146	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4147	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.

CVE-2016-4148	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4149	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4150	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4151	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4152	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4153	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4154	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4155	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4156	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash

	libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4160	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4120, CVE-2016-4161, CVE-2016-4162, and CVE-2016-4163.
CVE-2016-4161	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4120, CVE-2016-4160, CVE-2016-4162, and CVE-2016-4163.
CVE-2016-4162	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4120, CVE-2016-4160, CVE-2016-4161, and CVE-2016-4163.
CVE-2016-4163	Adobe Flash Player before 18.0.0.352 and 19.x through 21.x before 21.0.0.242 on Windows and OS X and before 11.2.202.621 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1096, CVE-2016-1098, CVE-2016-1099, CVE-2016-1100, CVE-2016-1102, CVE-2016-1104, CVE-2016-4109, CVE-2016-4111, CVE-2016-4112, CVE-2016-4113, CVE-2016-4114, CVE-2016-4115, CVE-2016-4120, CVE-2016-4160, CVE-2016-4161, and CVE-2016-4162.
CVE-2016-4166	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11

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

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

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

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

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

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

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

	CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4222	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4223	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2016-4224 and CVE-2016-4225.
CVE-2016-4224	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2016-4223 and CVE-2016-4225.
CVE-2016-4225	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2016-4223 and CVE-2016-4224.
CVE-2016-4226	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4227	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4228	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before

	11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4229	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4230	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4231	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, and CVE-2016-4248.
CVE-2016-4232	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to obtain sensitive information from process memory via unspecified vectors.
CVE-2016-4233	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236,

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

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

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

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

	CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, and CVE-2016-4246.
CVE-2016-4246	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4172, CVE-2016-4175, CVE-2016-4179, CVE-2016-4180, CVE-2016-4181, CVE-2016-4182, CVE-2016-4183, CVE-2016-4184, CVE-2016-4185, CVE-2016-4186, CVE-2016-4187, CVE-2016-4188, CVE-2016-4189, CVE-2016-4190, CVE-2016-4217, CVE-2016-4218, CVE-2016-4219, CVE-2016-4220, CVE-2016-4221, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, and CVE-2016-4245.
CVE-2016-4247	Race condition in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to obtain sensitive information via unspecified vectors.
CVE-2016-4248	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, and CVE-2016-4231.
CVE-2016-4249	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2016-4271	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, a different vulnerability than CVE-2016-4277 and CVE-2016-4278, aka a "local-with-filesystem Flash sandbox bypass" issue.
CVE-2016-4272	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different

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

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

	CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.
CVE-2016-4285	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-6922, and CVE-2016-6924.
CVE-2016-4286	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to bypass intended access restrictions via unspecified vectors.
CVE-2016-4287	Integer overflow in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2016-4429	Stack-based buffer overflow in the clntudp_call function in sunrpc/clnt_udp.c in the GNU C Library (aka glibc or libc6) allows remote servers to cause a denial of service (crash) or possibly unspecified other impact via a flood of crafted ICMP and UDP packets.
CVE-2016-5127	Use-after-free vulnerability in WebKit/Source/core/editing/VisibleUnits.cpp in Blink, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code involving an @import at-rule in a Cascading Style Sheets (CSS) token sequence in conjunction with a rel=import attribute of a LINK element.
CVE-2016-5128	objects.cc in Google V8 before 5.2.361.27, as used in Google Chrome before 52.0.2743.82, does not prevent API interceptors from modifying a store target without setting a property, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-5129	Google V8 before 5.2.361.32, as used in Google Chrome before 52.0.2743.82, does not properly process left-trimmed objects, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-5130	content/renderer/history_controller.cc in Google Chrome before 52.0.2743.82 does not properly restrict multiple uses of a JavaScript forward method, which

	allows remote attackers to spoof the URL display via a crafted web site.
CVE-2016-5131	Use-after-free vulnerability in libxml2 through 2.9.4, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the XPointer range-to function.
CVE-2016-5132	The Service Workers subsystem in Google Chrome before 52.0.2743.82 does not properly implement the Secure Contexts specification during decisions about whether to control a subframe, which allows remote attackers to bypass the Same Origin Policy via an https IFRAME element inside an http IFRAME element.
CVE-2016-5133	Google Chrome before 52.0.2743.82 mishandles origin information during proxy authentication, which allows man-in-the-middle attackers to spoof a proxy-authentication login prompt or trigger incorrect credential storage by modifying the client-server data stream.
CVE-2016-5134	net/proxy/proxy_service.cc in the Proxy Auto-Config (PAC) feature in Google Chrome before 52.0.2743.82 does not ensure that URL information is restricted to a scheme, host, and port, which allows remote attackers to discover credentials by operating a server with a PAC script, a related issue to CVE-2016-3763.
CVE-2016-5135	WebKit/Source/core/html/parser/HTMLPreloadScanner.cpp in Blink, as used in Google Chrome before 52.0.2743.82, does not consider referrer-policy information inside an HTML document during a preload request, which allows remote attackers to bypass the Content Security Policy (CSP) protection mechanism via a crafted web site, as demonstrated by a "Content-Security-Policy: referrer origin-when-cross-origin" header that overrides a "<META name='referrer' content='no-referrer'>" element.
CVE-2016-5136	Use-after-free vulnerability in extensions/renderer/user_script_injector.cc in the Extensions subsystem in Google Chrome before 52.0.2743.82 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to script deletion.
CVE-2016-5137	The CSPSource::schemeMatches function in WebKit/Source/core/frame/csp/CSPSource.cpp in the Content Security Policy (CSP) implementation in Blink, as used in Google Chrome before 52.0.2743.82, does not apply http :80 policies to https :443 URLs and does not apply ws :80 policies to wss :443 URLs, which makes it easier for remote attackers to determine whether a specific HSTS web site has been visited by reading a CSP

	report. NOTE: this vulnerability is associated with a specification change after CVE-2016-1617 resolution.
CVE-2016-5139	Multiple integer overflows in the opj_tcd_init_tile function in tcd.c in OpenJPEG, as used in PDFium in Google Chrome before 52.0.2743.116, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data.
CVE-2016-5140	Heap-based buffer overflow in the opj_j2k_read_SQcd_SQcc function in j2k.c in OpenJPEG, as used in PDFium in Google Chrome before 52.0.2743.116, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JPEG 2000 data.
CVE-2016-5141	Blink, as used in Google Chrome before 52.0.2743.116, allows remote attackers to spoof the address bar via vectors involving a provisional URL for an initially empty document, related to FrameLoader.cpp and ScopedPageLoadDeferrer.cpp.
CVE-2016-5142	The Web Cryptography API (aka WebCrypto) implementation in Blink, as used in Google Chrome before 52.0.2743.116, does not properly copy data buffers, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code, related to NormalizeAlgorithm.cpp and SubtleCrypto.cpp.
CVE-2016-5143	The Developer Tools (aka DevTools) subsystem in Blink, as used in Google Chrome before 52.0.2743.116, mishandles the script-path hostname, remoteBase parameter, and remoteFrontendUrl parameter, which allows remote attackers to bypass intended access restrictions via a crafted URL, a different vulnerability than CVE-2016-5144.
CVE-2016-5144	The Developer Tools (aka DevTools) subsystem in Blink, as used in Google Chrome before 52.0.2743.116, mishandles the script-path hostname, remoteBase parameter, and remoteFrontendUrl parameter, which allows remote attackers to bypass intended access restrictions via a crafted URL, a different vulnerability than CVE-2016-5143.
CVE-2016-5145	Blink, as used in Google Chrome before 52.0.2743.116, does not ensure that a taint property is preserved after a structure-clone operation on an ImageBitmap object derived from a cross-origin image, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.
CVE-2016-5146	Multiple unspecified vulnerabilities in Google Chrome before 52.0.2743.116 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.

CVE-2016-5147	Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, mishandles deferred page loads, which allows remote attackers to inject arbitrary web script or HTML via a crafted web site, aka "Universal XSS (UXSS)."
CVE-2016-5148	Cross-site scripting (XSS) vulnerability in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to inject arbitrary web script or HTML via vectors related to widget updates, aka "Universal XSS (UXSS)."
CVE-2016-5149	The extensions subsystem in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux relies on an IFRAME source URL to identify an associated extension, which allows remote attackers to conduct extension-bindings injection attacks by leveraging script access to a resource that initially has the about:blank URL.
CVE-2016-5150	WebKit/Source/bindings/modules/v8/V8BindingForModules.cpp in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, has an Indexed Database (aka IndexedDB) API implementation that does not properly restrict key-path evaluation, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code that leverages certain side effects.
CVE-2016-5151	PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux mishandles timers, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted PDF document, related to fpdfsdk/javascript/JS_Object.cpp and fpdfsdk/javascript/app.cpp.
CVE-2016-5152	Integer overflow in the opj_tcd_get_decoded_tile_size function in tcd.c in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data.
CVE-2016-5153	The Web Animations implementation in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, improperly relies on list iteration, which allows remote attackers to cause a denial of service (use-after-destruction) or possibly have unspecified other impact via a crafted web site.

CVE-2016-5154	Multiple heap-based buffer overflows in PDFium, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted JBig2 image.
CVE-2016-5155	Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly validate access to the initial document, which allows remote attackers to spoof the address bar via a crafted web site.
CVE-2016-5156	extensions/renderer/event_bindings.cc in the event bindings in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux attempts to process filtered events after failure to add an event matcher, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via unknown vectors.
CVE-2016-5157	Heap-based buffer overflow in the opj_dwt_interleave_v function in dwt.c in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to execute arbitrary code via crafted coordinate values in JPEG 2000 data.
CVE-2016-5158	Multiple integer overflows in the opj_tcd_init_tile function in tcd.c in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data.
CVE-2016-5159	Multiple integer overflows in OpenJPEG, as used in PDFium in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted JPEG 2000 data that is mishandled during opj_aligned_malloc calls in dwt.c and t1.c.
CVE-2016-5160	The AllowCrossRendererResourceLoad function in extensions/browser/url_request_util.cc in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly use an extension's manifest.json web_accessible_resources field for restrictions on IFRAME elements, which makes it easier for remote attackers to conduct clickjacking attacks, and trick users into changing extension settings, via a crafted web site, a different vulnerability than CVE-2016-5162.

CVE-2016-5161	The EditingStyle::mergeStyle function in WebKit/Source/core/editing/EditingStyle.cpp in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, mishandles custom properties, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site that leverages "type confusion" in the StylePropertySerializer class.
CVE-2016-5162	The AllowCrossRendererResourceLoad function in extensions/browser/url_request_util.cc in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly use an extension's manifest.json web_accessible_resources field for restrictions on IFRAME elements, which makes it easier for remote attackers to conduct clickjacking attacks, and trick users into changing extension settings, via a crafted web site, a different vulnerability than CVE-2016-5160.
CVE-2016-5163	The bidirectional-text implementation in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not ensure left-to-right (LTR) rendering of URLs, which allows remote attackers to spoof the address bar via crafted right-to-left (RTL) Unicode text, related to omnibox/SuggestionView.java and omnibox/UrlBar.java in Chrome for Android.
CVE-2016-5164	Cross-site scripting (XSS) vulnerability in WebKit/Source/platform/v8_inspector/V8Debugger.cpp in Blink, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, allows remote attackers to inject arbitrary web script or HTML into the Developer Tools (aka DevTools) subsystem via a crafted web site, aka "Universal XSS (UXSS)."
CVE-2016-5165	Cross-site scripting (XSS) vulnerability in the Developer Tools (aka DevTools) subsystem in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux allows remote attackers to inject arbitrary web script or HTML via the settings parameter in a chrome-devtools-frontend.appspot.com URL's query string.
CVE-2016-5166	The download implementation in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux does not properly restrict saving a file:// URL that is referenced by an http:// URL, which makes it easier for user-assisted remote attackers to discover NetNTLM hashes and conduct SMB relay attacks via a crafted web page that is accessed with the "Save page as" menu choice.
CVE-2016-5167	Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.89 on Windows and OS X and before

	53.0.2785.92 on Linux allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-5168	Skia, as used in Google Chrome before 50.0.2661.94, allows remote attackers to bypass the Same Origin Policy and obtain sensitive information.
CVE-2016-5170	WebKit/Source/bindings/modules/v8/V8BindingForModules.cpp in Blink, as used in Google Chrome before 53.0.2785.113, does not properly consider getter side effects during array key conversion, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted Indexed Database (aka IndexedDB) API calls.
CVE-2016-5171	WebKit/Source/bindings/templates/interface.cpp in Blink, as used in Google Chrome before 53.0.2785.113, does not prevent certain constructor calls, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-5172	The parser in Google V8, as used in Google Chrome before 53.0.2785.113, mishandles scopes, which allows remote attackers to obtain sensitive information from arbitrary memory locations via crafted JavaScript code.
CVE-2016-5173	The extensions subsystem in Google Chrome before 53.0.2785.113 does not properly restrict access to Object.prototype, which allows remote attackers to load unintended resources, and consequently trigger unintended JavaScript function calls and bypass the Same Origin Policy via an indirect interception attack.
CVE-2016-5174	browser/ui/cocoa/browser_window_controller_private.mm in Google Chrome before 53.0.2785.113 does not process fullscreen toggle requests during a fullscreen transition, which allows remote attackers to cause a denial of service (unsuppressed popup) via a crafted web site.
CVE-2016-5175	Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.113 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-5176	Google Chrome before 53.0.2785.113 allows remote attackers to bypass the SafeBrowsing protection mechanism via unspecified vectors.
CVE-2016-5177	Use-after-free vulnerability in V8 in Google Chrome before 53.0.2785.143 allows remote attackers to cause a denial of service (crash) or possibly have unspecified other impact via unknown vectors.
CVE-2016-5178	Multiple unspecified vulnerabilities in Google Chrome before 53.0.2785.143 allow remote attackers to cause

	a denial of service or possibly have other impact via unknown vectors.
CVE-2016-5181	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android permitted execution of v8 microtasks while the DOM was in an inconsistent state, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages.
CVE-2016-5182	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android had insufficient validation in bitmap handling, which allowed a remote attacker to potentially exploit heap corruption via crafted HTML pages.
CVE-2016-5183	A heap use after free in PDFium in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android allows a remote attacker to potentially exploit heap corruption via crafted PDF files.
CVE-2016-5184	PDFium in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object lifecycles in CFFL_FormFillter::KillFocusForAnnot, which allowed a remote attacker to potentially exploit heap corruption via crafted PDF files.
CVE-2016-5185	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly allowed reentrance of FrameView::updateLifecyclePhasesInternal(), which allowed a remote attacker to perform an out of bounds memory read via crafted HTML pages.
CVE-2016-5186	Devtools in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled objects after a tab crash, which allowed a remote attacker to perform an out of bounds memory read via crafted PDF files.
CVE-2016-5187	Google Chrome prior to 54.0.2840.85 for Android incorrectly handled rapid transition into and out of full screen mode, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages.
CVE-2016-5188	Multiple issues in Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux allow a remote attacker to spoof various parts of browser UI via crafted HTML pages.
CVE-2016-5189	Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android permitted navigation to blob URLs with non-canonical origins, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages.

CVE-2016-5190	Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object lifecycles during shutdown, which allowed a remote attacker to perform an out of bounds memory read via crafted HTML pages.
CVE-2016-5191	Bookmark handling in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android had insufficient validation of supplied data, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages, as demonstrated by an interpretation conflict between userinfo and scheme in an http://javascript:payload@example.com URL.
CVE-2016-5192	Blink in Google Chrome prior to 54.0.2840.59 for Windows missed a CORS check on redirect in TextTrackLoader, which allowed a remote attacker to bypass cross-origin restrictions via crafted HTML pages.
CVE-2016-5193	Google Chrome prior to 54.0 for iOS had insufficient validation of URLs for windows open by DOM, which allowed a remote attacker to bypass restrictions on navigation to certain URL schemes via crafted HTML pages.
CVE-2016-5194	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-5198	V8 in Google Chrome prior to 54.0.2840.90 for Linux, and 54.0.2840.85 for Android, and 54.0.2840.87 for Windows and Mac included incorrect optimisation assumptions, which allowed a remote attacker to perform arbitrary read/write operations, leading to code execution, via a crafted HTML page.
CVE-2016-5199	An off by one error resulting in an allocation of zero size in FFmpeg in Google Chrome prior to 54.0.2840.98 for Mac, and 54.0.2840.99 for Windows, and 54.0.2840.100 for Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2016-5200	V8 in Google Chrome prior to 54.0.2840.98 for Mac, and 54.0.2840.99 for Windows, and 54.0.2840.100 for Linux, and 55.0.2883.84 for Android incorrectly applied type rules, which allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5201	A leak of privateClass in the extensions API in Google Chrome prior to 54.0.2840.100 for Linux, and 54.0.2840.99 for Windows, and 54.0.2840.98 for

	Mac allowed a remote attacker to access privileged JavaScript code via a crafted HTML page.
CVE-2016-5202	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-5203	A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2016-5204	Leaking of an SVG shadow tree leading to corruption of the DOM tree in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2016-5205	Blink in Google Chrome prior to 55.0.2883.75 for Linux, Windows and Mac, incorrectly handles deferred page loads, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2016-5206	The PDF plugin in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly followed redirects, which allowed a remote attacker to bypass the Same Origin Policy via a crafted HTML page.
CVE-2016-5207	In Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android, corruption of the DOM tree could occur during the removal of a full screen element, which allowed a remote attacker to achieve arbitrary code execution via a crafted HTML page.
CVE-2016-5208	Blink in Google Chrome prior to 55.0.2883.75 for Linux and Windows, and 55.0.2883.84 for Android allowed possible corruption of the DOM tree during synchronous event handling, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2016-5209	Bad casting in bitmap manipulation in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5210	Heap buffer overflow during TIFF image parsing in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.

CVE-2016-5211	A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2016-5212	Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android insufficiently sanitized DevTools URLs, which allowed a remote attacker to read local files via a crafted HTML page.
CVE-2016-5213	A use after free in V8 in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5214	Google Chrome prior to 55.0.2883.75 for Windows mishandled downloaded files, which allowed a remote attacker to prevent the downloaded file from receiving the Mark of the Web via a crafted HTML page.
CVE-2016-5215	A use after free in webaudio in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2016-5216	A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2016-5217	The extensions API in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly permitted access to privileged plugins, which allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2016-5218	The extensions API in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled navigation within PDFs, which allowed a remote attacker to temporarily spoof the contents of the Omnibox (URL bar) via a crafted HTML page containing PDF data.
CVE-2016-5219	A heap use after free in V8 in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5220	PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled navigation within PDFs, which allowed a remote attacker to read local files via a crafted PDF file.

CVE-2016-5221	Type confusion in libGLESv2 in ANGLE in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android possibly allowed a remote attacker to bypass buffer validation via a crafted HTML page.
CVE-2016-5222	Incorrect handling of invalid URLs in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2016-5223	Integer overflow in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption or DoS via a crafted PDF file.
CVE-2016-5224	A timing attack on denormalized floating point arithmetic in SVG filters in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to bypass the Same Origin Policy via a crafted HTML page.
CVE-2016-5225	Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled form actions, which allowed a remote attacker to bypass Content Security Policy via a crafted HTML page.
CVE-2016-5226	Blink in Google Chrome prior to 55.0.2883.75 for Linux, Windows and Mac executed javascript: URLs entered in the URL bar in the context of the current tab, which allowed a socially engineered user to XSS themselves by dragging and dropping a javascript: URL into the URL bar.
CVE-2016-6921	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4272, CVE-2016-4279, CVE-2016-6923, CVE-2016-6925, CVE-2016-6926, CVE-2016-6927, CVE-2016-6929, CVE-2016-6930, CVE-2016-6931, and CVE-2016-6932.
CVE-2016-6922	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-4285, and CVE-2016-6924.

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

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

	CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, CVE-2016-6989, and CVE-2016-6990.
CVE-2016-6984	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4273, CVE-2016-6982, CVE-2016-6983, CVE-2016-6985, CVE-2016-6986, CVE-2016-6989, and CVE-2016-6990.
CVE-2016-6985	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4273, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6986, CVE-2016-6989, and CVE-2016-6990.
CVE-2016-6986	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4273, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6989, and CVE-2016-6990.
CVE-2016-6987	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-6981.
CVE-2016-6989	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4273, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, and CVE-2016-6990.
CVE-2016-6990	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4273, CVE-2016-6982, CVE-2016-6983, CVE-2016-6984, CVE-2016-6985, CVE-2016-6986, and CVE-2016-6989.
CVE-2016-6992	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to

	execute arbitrary code by leveraging an unspecified "type confusion."
CVE-2016-7020	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-7395	SkPath.cpp in Skia, as used in Google Chrome before 53.0.2785.89 on Windows and OS X and before 53.0.2785.92 on Linux, does not properly validate the return values of ChopMonoAtY calls, which allows remote attackers to cause a denial of service (uninitialized memory access and application crash) or possibly have unspecified other impact via crafted graphics data.
CVE-2016-7549	Google Chrome before 53.0.2785.113 does not ensure that the recipient of a certain IPC message is a valid RenderFrame or RenderWidget, which allows remote attackers to cause a denial of service (invalid pointer dereference and application crash) or possibly have unspecified other impact by leveraging access to a renderer process, related to render_frame_host_impl.cc and render_widget_host_impl.cc, as demonstrated by a Password Manager message.
CVE-2016-7855	Use-after-free vulnerability in Adobe Flash Player before 23.0.0.205 on Windows and OS X and before 11.2.202.643 on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in October 2016.
CVE-2016-7857	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7858	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7859	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7860	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.

CVE-2016-7861	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7862	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7863	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7864	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable use-after-free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7865	Adobe Flash Player versions 23.0.0.205 and earlier, 11.2.202.643 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7867	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class related to bookmarking in searches. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7868	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class related to alternation functionality. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7869	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class related to backtrack search functionality. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7870	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable buffer overflow / underflow vulnerability in the RegExp class for specific search strategies. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7871	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulnerability in the Worker class. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7872	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the MovieClip class related to objects at multiple presentation levels. Successful exploitation could lead to arbitrary code execution.

CVE-2016-7873	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulnerability in the PSDK class related to ad policy functionality method. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7874	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulnerability in the NetConnection class when handling the proxy types. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7875	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable integer overflow vulnerability in the BitmapData class. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7876	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable memory corruption vulnerability in the Clipboard class related to data handling functionality. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7877	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the Action Message Format serialization (AFM0). Successful exploitation could lead to arbitrary code execution.
CVE-2016-7878	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the PSDK's MediaPlayer class. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7879	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the NetConnection class when handling an attached script object. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7880	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability when setting the length property of an array object. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7881	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the MovieClip class when handling conversion to an object. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7890	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have security bypass vulnerability in the implementation of the same origin policy.

CVE-2016-7892	Adobe Flash Player versions 23.0.0.207 and earlier, 11.2.202.644 and earlier have an exploitable use after free vulnerability in the TextField class. Successful exploitation could lead to arbitrary code execution.
CVE-2016-7942	The XGetImage function in X.org libX11 before 1.6.4 might allow remote X servers to gain privileges via vectors involving image type and geometry, which triggers out-of-bounds read operations.
CVE-2016-7943	The XListFonts function in X.org libX11 before 1.6.4 might allow remote X servers to gain privileges via vectors involving length fields, which trigger out-of-bounds write operations.
CVE-2016-9318	libxml2 2.9.4 and earlier, as used in XMLSec 1.2.23 and earlier and other products, does not offer a flag directly indicating that the current document may be read but other files may not be opened, which makes it easier for remote attackers to conduct XML External Entity (XXE) attacks via a crafted document.
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	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-9652	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2017-1000242	Jenkins Git Client Plugin 2.4.2 and earlier creates temporary file with insecure permissions resulting in information disclosure
CVE-2017-1000445	ImageMagick 7.0.7-1 and older version are vulnerable to null pointer dereference in the MagickCore component and might lead to denial of service
CVE-2017-1000476	ImageMagick 7.0.7-12 Q16, a CPU exhaustion vulnerability was found in the function ReadDDSInfo in coders/dds.c, which allows attackers to cause a denial of service.
CVE-2017-10995	The mng_get_long function in coders/png.c in ImageMagick 7.0.6-0 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted MNG image.
CVE-2017-11213	An issue was discovered in Adobe Flash Player 27.0.0.183 and earlier versions. This vulnerability

	occurs as a result of a computation that reads data that is past the end of the target buffer due to an integer overflow; the computation is part of the abstraction that creates an arbitrarily sized transparent or opaque bitmap image. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure.
CVE-2017-11215	An issue was discovered in Adobe Flash Player 27.0.0.183 and earlier versions. This vulnerability is an instance of a use after free vulnerability in the Primetime SDK. The mismatch between an old and a new object can provide an attacker with unintended memory access -- potentially leading to code corruption, control-flow hijack, or an information leak attack. Successful exploitation could lead to arbitrary code execution.
CVE-2017-11225	An issue was discovered in Adobe Flash Player 27.0.0.183 and earlier versions. This vulnerability is an instance of a use after free vulnerability in the Primetime SDK metadata functionality. The mismatch between an old and a new object can provide an attacker with unintended memory access -- potentially leading to code corruption, control-flow hijack, or an information leak attack. Successful exploitation could lead to arbitrary code execution.
CVE-2017-11281	Adobe Flash Player has an exploitable memory corruption vulnerability in the text handling function. Successful exploitation could lead to arbitrary code execution. This affects 26.0.0.151 and earlier.
CVE-2017-11282	Adobe Flash Player has an exploitable memory corruption vulnerability in the MP4 atom parser. Successful exploitation could lead to arbitrary code execution. This affects 26.0.0.151 and earlier.
CVE-2017-11292	Adobe Flash Player version 27.0.0.159 and earlier has a flawed bytecode verification procedure, which allows for an untrusted value to be used in the calculation of an array index. This can lead to type confusion, and successful exploitation could lead to arbitrary code execution.
CVE-2017-11352	In ImageMagick before 7.0.5-10, a crafted RLE image can trigger a crash because of incorrect EOF handling in coders/rle.c. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-9144.
CVE-2017-11533	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a heap-based buffer over-read in the WriteUILImage() function in coders/uil.c.
CVE-2017-11535	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a heap-based buffer over-read in the WritePSImage() function in coders/ps.c.

CVE-2017-11537	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Floating Point Exception (FPE) in the WritePALMImage() function in coders/palm.c, related to an incorrect bits-per-pixel calculation.
CVE-2017-11639	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a heap-based buffer over-read in the WriteCIPImage() function in coders/cip.c, related to the GetPixelLuma function in MagickCore/pixel-accessor.h.
CVE-2017-11640	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to an address access exception in the WritePTIFImage() function in coders/tiff.c.
CVE-2017-12140	The ReadDCMImage function in coders\dcm.c in ImageMagick 7.0.6-1 has an integer signedness error leading to excessive memory consumption via a crafted DCM file.
CVE-2017-12194	A flaw was found in the way spice-client processed certain messages sent from the server. An attacker, having control of malicious spice-server, could use this flaw to crash the client or execute arbitrary code with permissions of the user running the client. spice-gtk versions through 0.34 are believed to be vulnerable.
CVE-2017-12418	ImageMagick 7.0.6-5 has memory leaks in the parse8BIMW and format8BIM functions in coders/meta.c, related to the WriteImage function in MagickCore/constitute.c.
CVE-2017-12429	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadMIFFImage in coders/miff.c, which allows attackers to cause a denial of service.
CVE-2017-12430	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadMPCImage in coders/mpc.c, which allows attackers to cause a denial of service.
CVE-2017-12431	In ImageMagick 7.0.6-1, a use-after-free vulnerability was found in the function ReadWMFImage in coders/wmf.c, which allows attackers to cause a denial of service.
CVE-2017-12432	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadPCXImage in coders/pcx.c, which allows attackers to cause a denial of service.
CVE-2017-12433	In ImageMagick 7.0.6-1, a memory leak vulnerability was found in the function ReadPESImage in coders/pes.c, which allows attackers to cause a denial of service, related to ResizeMagickMemory in memory.c.
CVE-2017-12435	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadSUNImage

	in coders/sun.c, which allows attackers to cause a denial of service.
CVE-2017-12563	In ImageMagick 7.0.6-2, a memory exhaustion vulnerability was found in the function ReadPSDImage in coders/psd.c, which allows attackers to cause a denial of service.
CVE-2017-12587	ImageMagick 7.0.6-1 has a large loop vulnerability in the ReadPWPImage function in coders\pwp.c.
CVE-2017-12616	When using a VirtualDirContext with Apache Tomcat 7.0.0 to 7.0.80 it was possible to bypass security constraints and/or view the source code of JSPs for resources served by the VirtualDirContext using a specially crafted request.
CVE-2017-12617	When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default servlet to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.
CVE-2017-12640	ImageMagick 7.0.6-1 has an out-of-bounds read vulnerability in ReadOneMNGImage in coders/png.c.
CVE-2017-12643	ImageMagick 7.0.6-1 has a memory exhaustion vulnerability in ReadOneJNGImage in coders\png.c.
CVE-2017-12644	ImageMagick 7.0.6-1 has a memory leak vulnerability in ReadDCMImage in coders\dcm.c.
CVE-2017-12670	In ImageMagick 7.0.6-3, missing validation was found in coders/mat.c, leading to an assertion failure in the function DestroyImage in MagickCore/image.c, which allows attackers to cause a denial of service.
CVE-2017-12674	In ImageMagick 7.0.6-2, a CPU exhaustion vulnerability was found in the function ReadPDBImage in coders/pdb.c, which allows attackers to cause a denial of service.
CVE-2017-12691	The ReadOneLayer function in coders/xcf.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted file.
CVE-2017-12692	The ReadVIFFImage function in coders/viff.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted VIFF file.
CVE-2017-12693	The ReadBMPImage function in coders/bmp.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted BMP file.

CVE-2017-12875	The WritePixelCachePixels function in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (CPU consumption) via a crafted file.
CVE-2017-12877	Use-after-free vulnerability in the DestroyImage function in image.c in ImageMagick before 7.0.6-6 allows remote attackers to cause a denial of service via a crafted file.
CVE-2017-12983	Heap-based buffer overflow in the ReadSFWImage function in coders/sfw.c in ImageMagick 7.0.6-8 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file.
CVE-2017-13058	In ImageMagick 7.0.6-6, a memory leak vulnerability was found in the function WritePCXImage in coders/pcx.c, which allows attackers to cause a denial of service via a crafted file.
CVE-2017-13059	In ImageMagick 7.0.6-6, a memory leak vulnerability was found in the function WriteOneJNGImage in coders/png.c, which allows attackers to cause a denial of service (WriteJNGImage memory consumption) via a crafted file.
CVE-2017-13060	In ImageMagick 7.0.6-5, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service via a crafted file.
CVE-2017-13061	In ImageMagick 7.0.6-5, a length-validation vulnerability was found in the function ReadPSDLayersInternal in coders/psd.c, which allows attackers to cause a denial of service (ReadPSDImage memory exhaustion) via a crafted file.
CVE-2017-13062	In ImageMagick 7.0.6-6, a memory leak vulnerability was found in the function formatIPTC in coders/meta.c, which allows attackers to cause a denial of service (WriteMETAImage memory consumption) via a crafted file.
CVE-2017-13131	In ImageMagick 7.0.6-8, a memory leak vulnerability was found in the function ReadMIFFImage in coders/miff.c, which allows attackers to cause a denial of service (memory consumption in NewLinkedList in MagickCore/linked-list.c) via a crafted file.
CVE-2017-13134	In ImageMagick 7.0.6-6 and GraphicsMagick 1.3.26, a heap-based buffer over-read was found in the function SFWScan in coders/sfw.c, which allows attackers to cause a denial of service via a crafted file.
CVE-2017-13139	In ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1, the ReadOneMNGImage function in coders/png.c has an out-of-bounds read with the MNG CLIP chunk.
CVE-2017-13142	In ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1, a crafted PNG file could trigger a crash because there was an insufficient check for short files.

CVE-2017-13143	In ImageMagick before 6.9.7-6 and 7.x before 7.0.4-6, the ReadMATImage function in coders/mat.c uses uninitialized data, which might allow remote attackers to obtain sensitive information from process memory.
CVE-2017-13144	In ImageMagick before 6.9.7-10, there is a crash (rather than a "width or height exceeds limit" error report) if the image dimensions are too large, as demonstrated by use of the mpc coder.
CVE-2017-13145	In ImageMagick before 6.9.8-8 and 7.x before 7.0.5-9, the ReadJP2Image function in coders/jp2.c does not properly validate the channel geometry, leading to a crash.
CVE-2017-13695	The acpi_ns_evaluate() function in drivers/acpi/acpica/nseval.c in the Linux kernel through 4.12.9 does not flush the operand cache and causes a kernel stack dump, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism (in the kernel through 4.9) via a crafted ACPI table.
CVE-2017-13758	In ImageMagick 7.0.6-10, there is a heap-based buffer overflow in the TracePoint() function in MagickCore/draw.c.
CVE-2017-13768	Null Pointer Dereference in the IdentifyImage function in MagickCore/identify.c in ImageMagick through 7.0.6-10 allows an attacker to perform denial of service by sending a crafted image file.
CVE-2017-13769	The WriteTHUMBNAILImage function in coders/thumbnail.c in ImageMagick through 7.0.6-10 allows an attacker to cause a denial of service (buffer over-read) by sending a crafted JPEG file.
CVE-2017-14060	In ImageMagick 7.0.6-10, a NULL Pointer Dereference issue is present in the ReadCUTImage function in coders/cut.c that could allow an attacker to cause a Denial of Service (in the QueueAuthenticPixelCacheNexus function within the MagickCore/cache.c file) by submitting a malformed image file.
CVE-2017-14172	In coders/ps.c in ImageMagick 7.0.7-0 Q16, a DoS in ReadPSImage() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted PSD file, which claims a large "extent" field in the header but does not contain sufficient backing data, is provided, the loop over "length" would consume huge CPU resources, since there is no EOF check inside the loop.
CVE-2017-14173	In the function ReadTXTImage() in coders/txt.c in ImageMagick 7.0.6-10, an integer overflow might occur for the addition operation "GetQuantumRange(depth)+1" when "depth" is large, producing a smaller value than expected. As a result,

	an infinite loop would occur for a crafted TXT file that claims a very large "max_value" value.
CVE-2017-14174	In coders/psd.c in ImageMagick 7.0.7-0 Q16, a DoS in ReadPSDLayersInternal() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted PSD file, which claims a large "length" field in the header but does not contain sufficient backing data, is provided, the loop over "length" would consume huge CPU resources, since there is no EOF check inside the loop.
CVE-2017-14175	In coders/xbm.c in ImageMagick 7.0.6-1 Q16, a DoS in ReadXBMImage() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted XBM file, which claims large rows and columns fields in the header but does not contain sufficient backing data, is provided, the loop over the rows would consume huge CPU resources, since there is no EOF check inside the loop.
CVE-2017-14224	A heap-based buffer overflow in WritePCXImage in coders/pcx.c in ImageMagick 7.0.6-8 Q16 allows remote attackers to cause a denial of service or code execution via a crafted file.
CVE-2017-14249	ImageMagick 7.0.6-8 Q16 mishandles EOF checks in ReadMPCImage in coders/mpc.c, leading to division by zero in GetPixelCacheTileSize in MagickCore/cache.c, allowing remote attackers to cause a denial of service via a crafted file.
CVE-2017-14325	In ImageMagick 7.0.7-1 Q16, a memory leak vulnerability was found in the function PersistPixelCache in magick/cache.c, which allows attackers to cause a denial of service (memory consumption in ReadMPCImage in coders/mpc.c) via a crafted file.
CVE-2017-14326	In ImageMagick 7.0.7-1 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service via a crafted file.
CVE-2017-14341	ImageMagick 7.0.6-6 has a large loop vulnerability in ReadWPGImage in coders/wpg.c, causing CPU exhaustion via a crafted wpg image file.
CVE-2017-14342	ImageMagick 7.0.6-6 has a memory exhaustion vulnerability in ReadWPGImage in coders/wpg.c via a crafted wpg image file.
CVE-2017-14343	ImageMagick 7.0.6-6 has a memory leak vulnerability in ReadXCFImage in coders/xcf.c via a crafted xcf image file.
CVE-2017-14400	In ImageMagick 7.0.7-1 Q16, the PersistPixelCache function in magick/cache.c mishandles the pixel cache nexus, which allows remote attackers to cause a denial

	of service (NULL pointer dereference in the function GetVirtualPixels in MagickCore/cache.c) via a crafted file.
CVE-2017-14501	An out-of-bounds read flaw exists in parse_file_info in archive_read_support_format_iso9660.c in libarchive 3.3.2 when extracting a specially crafted iso9660 iso file, related to archive_read_format_iso9660_read_header.
CVE-2017-14503	libarchive 3.3.2 suffers from an out-of-bounds read within lha_read_data_none() in archive_read_support_format_lha.c when extracting a specially crafted lha archive, related to lha_crc16.
CVE-2017-14505	DrawGetStrokeDashArray in wand/drawing-wand.c in ImageMagick 7.0.7-1 mishandles certain NULL arrays, which allows attackers to perform Denial of Service (NULL pointer dereference and application crash in AcquireQuantumMemory within MagickCore/memory.c) by providing a crafted Image File as input.
CVE-2017-14531	ImageMagick 7.0.7-0 has a memory exhaustion issue in ReadSUNImage in coders/sun.c.
CVE-2017-14532	ImageMagick 7.0.7-0 has a NULL Pointer Dereference in TIFFIgnoreTags in coders/tiff.c.
CVE-2017-14533	ImageMagick 7.0.6-6 has a memory leak in ReadMATImage in coders/mat.c.
CVE-2017-14607	In ImageMagick 7.0.7-4 Q16, an out of bounds read flaw related to ReadTIFFImage has been reported in coders/tiff.c. An attacker could possibly exploit this flaw to disclose potentially sensitive memory or cause an application crash.
CVE-2017-14624	ImageMagick 7.0.7-0 Q16 has a NULL Pointer Dereference vulnerability in the function PostscriptDelegateMessage in coders/ps.c.
CVE-2017-14625	ImageMagick 7.0.7-0 Q16 has a NULL Pointer Dereference vulnerability in the function sixel_output_create in coders/sixel.c.
CVE-2017-14626	ImageMagick 7.0.7-0 Q16 has a NULL Pointer Dereference vulnerability in the function sixel_decode in coders/sixel.c.
CVE-2017-14682	GetNextToken in MagickCore/token.c in ImageMagick 7.0.6 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 SVG document, a different vulnerability than CVE-2017-10928.
CVE-2017-14684	In ImageMagick 7.0.7-4 Q16, a memory leak vulnerability was found in the function ReadVIPSImage in coders/vips.c, which allows attackers to cause a denial of service (memory consumption in

	ResizeMagickMemory in MagickCore/memory.c) via a crafted file.
CVE-2017-14739	The AcquireResampleFilterThreadSet function in magick/resample-private.h in ImageMagick 7.0.7-4 mishandles failed memory allocation, which allows remote attackers to cause a denial of service (NULL Pointer Dereference in DistortImage in MagickCore/distort.c, and application crash) via unspecified vectors.
CVE-2017-14741	The ReadCAPTIONImage function in coders/caption.c in ImageMagick 7.0.7-3 allows remote attackers to cause a denial of service (infinite loop) via a crafted font file.
CVE-2017-14989	A use-after-free in RenderFreetype in MagickCore/annotate.c in ImageMagick 7.0.7-4 Q16 allows attackers to crash the application via a crafted font file, because the FT_Done_Glyph function (from FreeType 2) is called at an incorrect place in the ImageMagick code.
CVE-2017-15015	ImageMagick 7.0.7-0 Q16 has a NULL pointer dereference vulnerability in PDFDelegateMessage in coders/pdf.c.
CVE-2017-15016	ImageMagick 7.0.7-0 Q16 has a NULL pointer dereference vulnerability in ReadEnhMetaFile in coders/emf.c.
CVE-2017-15017	ImageMagick 7.0.7-0 Q16 has a NULL pointer dereference vulnerability in ReadOneMNGImage in coders/png.c.
CVE-2017-15032	ImageMagick version 7.0.7-2 contains a memory leak in ReadYCBCRImage in coders/ycbcr.c.
CVE-2017-15033	ImageMagick version 7.0.7-2 contains a memory leak in ReadYUVImage in coders/yuv.c.
CVE-2017-15105	A flaw was found in the way unbound before 1.6.8 validated wildcard-synthesized NSEC records. An improperly validated wildcard NSEC record could be used to prove the non-existence (NXDOMAIN answer) of an existing wildcard record, or trick unbound into accepting a NODATA proof.
CVE-2017-15217	ImageMagick 7.0.7-2 has a memory leak in ReadSGIImage in coders/sgi.c.
CVE-2017-15218	ImageMagick 7.0.7-2 has a memory leak in ReadOneJNGImage in coders/png.c.
CVE-2017-15232	libjpeg-turbo 1.5.2 has a NULL Pointer Dereference in jdpostct.c and jquant1.c via a crafted JPEG file.
CVE-2017-15277	ReadGIFImage in coders/gif.c in ImageMagick 7.0.6-1 and GraphicsMagick 1.3.26 leaves the palette uninitialized when processing a GIF file that has neither a global nor local palette. If the affected product is used as a library loaded into a process that operates on

	interesting data, this data sometimes can be leaked via the uninitialized palette.
CVE-2017-15281	ReadPSDImage in coders/psd.c in ImageMagick 7.0.7-6 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file, related to "Conditional jump or move depends on uninitialised value(s)."
CVE-2017-15386	Incorrect implementation in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-15387	Insufficient enforcement of Content Security Policy in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to open javascript: URL windows when they should not be allowed to via a crafted HTML page.
CVE-2017-15388	Iteration through non-finite points in Skia in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-15389	An insufficient watchdog timer in navigation in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-15390	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-15391	Insufficient Policy Enforcement in Extensions in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to access Extension pages without authorisation via a crafted HTML page.
CVE-2017-15392	Insufficient data validation in V8 in Google Chrome prior to 62.0.3202.62 allowed an attacker who can write to the Windows Registry to potentially exploit heap corruption via a crafted Windows Registry entry, related to PlatformIntegration.
CVE-2017-15393	Insufficient Policy Enforcement in Devtools remote debugging in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to obtain access to remote debugging functionality via a crafted HTML page, aka a Referer leak.
CVE-2017-15394	Insufficient Policy Enforcement in Extensions in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform domain spoofing in permission dialogs via IDN homographs in a crafted Chrome Extension.
CVE-2017-15395	A use after free in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka an ImageCapture NULL pointer dereference.

CVE-2017-15396	A stack buffer overflow in NumberingSystem in International Components for Unicode (ICU) for C/C++ before 60.2, as used in V8 in Google Chrome prior to 62.0.3202.75 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-15398	A stack buffer overflow in the QUIC networking stack in Google Chrome prior to 62.0.3202.89 allowed a remote attacker to gain code execution via a malicious server.
CVE-2017-15399	A use after free in V8 in Google Chrome prior to 62.0.3202.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-15406	A stack buffer overflow in V8 in Google Chrome prior to 62.0.3202.75 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-15407	Out-of-bounds Write in the QUIC networking stack in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to gain code execution via a malicious server.
CVE-2017-15408	Heap buffer overflow in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file that is mishandled by PDFium.
CVE-2017-15409	Heap buffer overflow in Skia in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-15410	Use after free in PDFium in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-15411	Use after free in PDFium in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-15412	Use after free in libxml2 before 2.9.5, as used in Google Chrome prior to 63.0.3239.84 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-15413	Type confusion in WebAssembly in V8 in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-15415	Incorrect serialization in IPC in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to leak the value of a pointer via a crafted HTML page.
CVE-2017-15416	Heap buffer overflow in Blob API in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka a Blink out-of-bounds read.
CVE-2017-15417	Inappropriate implementation in Skia canvas composite operations in Google Chrome prior to 63.0.3239.84

	allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2017-15418	Use of uninitialized memory in Skia in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-15419	Insufficient policy enforcement in Resource Timing API in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to infer browsing history by triggering a leaked cross-origin URL via a crafted HTML page.
CVE-2017-15420	Inappropriate implementation in browser navigation in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-15422	Integer overflow in international date handling in International Components for Unicode (ICU) for C/C++ before 60.1, as used in V8 in Google Chrome prior to 63.0.3239.84 and other products, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-15423	Inappropriate implementation in BoringSSL SPAKE2 in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to leak the low-order bits of SHA512(password) by inspecting protocol traffic.
CVE-2017-15424	Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-15425	Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-15426	Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-15427	Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a socially engineered user to XSS themselves by dragging and dropping a javascript: URL into the URL bar.
CVE-2017-15429	Inappropriate implementation in V8 WebAssembly JS bindings in Google Chrome prior to 63.0.3239.108 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-15430	Unsafe navigation in Chromecast in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2017-15705	A denial of service vulnerability was identified that exists in Apache SpamAssassin before 3.4.2. The

	vulnerability arises with certain unclosed tags in emails that cause markup to be handled incorrectly leading to scan timeouts. In Apache SpamAssassin, using HTML::Parser, we setup an object and hook into the begin and end tag event handlers In both cases, the "open" event is immediately followed by a "close" event - even if the tag *does not* close in the HTML being parsed. Because of this, we are missing the "text" event to deal with the object normally. This can cause carefully crafted emails that might take more scan time than expected leading to a Denial of Service. The issue is possibly a bug or design decision in HTML::Parser that specifically impacts the way Apache SpamAssassin uses the module with poorly formed html. The exploit has been seen in the wild but not believed to have been purposefully part of a Denial of Service attempt. We are concerned that there may be attempts to abuse the vulnerability in the future.
CVE-2017-15706	As part of the fix for bug 61201, the documentation for Apache Tomcat 9.0.0.M22 to 9.0.1, 8.5.16 to 8.5.23, 8.0.45 to 8.0.47 and 7.0.79 to 7.0.82 included an updated description of the search algorithm used by the CGI Servlet to identify which script to execute. The update was not correct. As a result, some scripts may have failed to execute as expected and other scripts may have been executed unexpectedly. Note that the behaviour of the CGI servlet has remained unchanged in this regard. It is only the documentation of the behaviour that was wrong and has been corrected.
CVE-2017-15710	In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.
CVE-2017-15715	In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.

CVE-2017-16546	The ReadWPGImage function in coders/wpg.c in ImageMagick 7.0.7-9 does not properly validate the colormap index in a WPG palette, which allows remote attackers to cause a denial of service (use of uninitialized data or invalid memory allocation) or possibly have unspecified other impact via a malformed WPG file.
CVE-2017-16845	hw/input/ps2.c in Qemu does not validate 'rptr' and 'count' values during guest migration, leading to out-of-bounds access.
CVE-2017-16932	parser.c in libxml2 before 2.9.5 does not prevent infinite recursion in parameter entities.
CVE-2017-17499	ImageMagick before 6.9.9-24 and 7.x before 7.0.7-12 has a use-after-free in Magick::Image::read in Magick++/lib/Image.cpp.
CVE-2017-17504	ImageMagick before 7.0.7-12 has a coders/png.c Magick_png_read_raw_profile heap-based buffer over-read via a crafted file, related to ReadOneMNGImage.
CVE-2017-17680	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadXPMImage in coders/xpm.c, which allows attackers to cause a denial of service via a crafted xpm image file.
CVE-2017-17681	In ImageMagick 7.0.7-12 Q16, an infinite loop vulnerability was found in the function ReadPSDChannelZip in coders/psd.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted psd image file.
CVE-2017-17682	In ImageMagick 7.0.7-12 Q16, a large loop vulnerability was found in the function ExtractPostscript in coders/wpg.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted wpg image file that triggers a ReadWPGImage call.
CVE-2017-17879	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-21, there is a heap-based buffer over-read in ReadOneMNGImage in coders/png.c, related to length calculation and caused by an off-by-one error.
CVE-2017-17881	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service via a crafted MAT image file.
CVE-2017-17882	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadXPMImage in coders/xpm.c, which allows attackers to cause a denial of service via a crafted XPM image file.
CVE-2017-17884	In ImageMagick 7.0.7-16 Q16, a memory leak vulnerability was found in the function WriteOnePNGImage in coders/png.c, which allows attackers to cause a denial of service via a crafted PNG image file.

CVE-2017-17885	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadPICTImage in coders/pict.c, which allows attackers to cause a denial of service via a crafted PICT image file.
CVE-2017-17886	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadPSDChannelZip in coders/psd.c, which allows attackers to cause a denial of service via a crafted psd image file.
CVE-2017-17887	In ImageMagick 7.0.7-16 Q16, a memory leak vulnerability was found in the function GetImagePixelCache in magick/cache.c, which allows attackers to cause a denial of service via a crafted MNG image file that is processed by ReadOneMNGImage.
CVE-2017-17914	In ImageMagick 7.0.7-16 Q16, a vulnerability was found in the function ReadOnePNGImage in coders/png.c, which allows attackers to cause a denial of service (ReadOneMNGImage large loop) via a crafted mng image file.
CVE-2017-17934	ImageMagick 7.0.7-17 Q16 x86_64 has memory leaks in coders/msl.c, related to MSLPopImage and ProcessMSLScript, and associated with mishandling of MSLPushImage calls.
CVE-2017-18008	In ImageMagick 7.0.7-17 Q16, there is a Memory Leak in ReadPWPImage in coders/pwp.c.
CVE-2017-18022	In ImageMagick 7.0.7-12 Q16, there are memory leaks in MontageImageCommand in MagickWand/montage.c.
CVE-2017-18027	In ImageMagick 7.0.7-1 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allow remote attackers to cause a denial of service via a crafted file.
CVE-2017-18028	In ImageMagick 7.0.7-1 Q16, a memory exhaustion vulnerability was found in the function ReadTIFFImage in coders/tiff.c, which allow remote attackers to cause a denial of service via a crafted file.
CVE-2017-18029	In ImageMagick 7.0.6-10 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allow remote attackers to cause a denial of service via a crafted file.
CVE-2017-18209	In the GetOpenCLCachedFilesDirectory function in magick/opencl.c in ImageMagick 7.0.7, a NULL pointer dereference vulnerability occurs because a memory allocation result is not checked, related to GetOpenCLCacheDirectory.
CVE-2017-18211	In ImageMagick 7.0.7, a NULL pointer dereference vulnerability was found in the function saveBinaryCLProgram in magick/opencl.c because a program-lookup result is not checked, related to CacheOpenCLKernel.

CVE-2017-18248	The add_job function in scheduler/ipp.c in CUPS before 2.2.6, when D-Bus support is enabled, can be crashed by remote attackers by sending print jobs with an invalid username, related to a D-Bus notification.
CVE-2017-18251	An issue was discovered in ImageMagick 7.0.7. A memory leak vulnerability was found in the function ReadPCDImage in coders/pcd.c, which allow remote attackers to cause a denial of service via a crafted file.
CVE-2017-18252	An issue was discovered in ImageMagick 7.0.7. The MogrifyImageList function in MagickWand/mogrify.c allows attackers to cause a denial of service (assertion failure and application exit in ReplaceImageInList) via a crafted file.
CVE-2017-18254	An issue was discovered in ImageMagick 7.0.7. A memory leak vulnerability was found in the function WriteGIFImage in coders/gif.c, which allow remote attackers to cause a denial of service via a crafted file.
CVE-2017-18258	The xz_head function in xzlib.c in libxml2 before 2.9.6 allows remote attackers to cause a denial of service (memory consumption) via a crafted LZMA file, because the decoder functionality does not restrict memory usage to what is required for a legitimate file.
CVE-2017-18266	The open_envvar function in xdg-open in xdg-utils before 1.1.3 does not validate strings before launching the program specified by the BROWSER environment variable, which might allow remote attackers to conduct argument-injection attacks via a crafted URL, as demonstrated by %s in this environment variable.
CVE-2017-18267	The FoFiType1C::cvtGlyph function in fofi/FoFiType1C.cc in Poppler through 0.64.0 allows remote attackers to cause a denial of service (infinite recursion) via a crafted PDF file, as demonstrated by pdftops.
CVE-2017-18271	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-22, an infinite loop vulnerability was found in the function ReadMIFFImage in coders/miff.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted MIFF image file.
CVE-2017-18273	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-22, an infinite loop vulnerability was found in the function ReadTXTImage in coders/txt.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted image file that is mishandled in a GetImageIndexInList call.
CVE-2017-2925	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable memory corruption vulnerability in the JPEG XR codec. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2926	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable memory corruption vulnerability

	related to processing of atoms in MP4 files. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2927	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable heap overflow vulnerability when processing Adobe Texture Format files. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2928	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable memory corruption vulnerability related to setting visual mode effects. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2930	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable memory corruption vulnerability due to a concurrency error when manipulating a display list. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2931	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable memory corruption vulnerability related to the parsing of SWF metadata. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2932	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable use after free vulnerability in the ActionScript MovieClip class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2933	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable heap overflow vulnerability related to texture compression. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2934	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable heap overflow vulnerability when parsing Adobe Texture Format files. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2935	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable heap overflow vulnerability when processing the Flash Video container file format. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2936	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable use after free vulnerability in the ActionScript FileReference class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2937	Adobe Flash Player versions 24.0.0.186 and earlier have an exploitable use after free vulnerability in the ActionScript FileReference class, when using class inheritance. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2938	Adobe Flash Player versions 24.0.0.186 and earlier have a security bypass vulnerability related to handling TCP connections.

CVE-2017-2982	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability in a routine related to player shutdown. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2984	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable heap overflow vulnerability in the h264 decoder routine. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2985	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability in the ActionScript 3 BitmapData class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2986	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable heap overflow vulnerability in the Flash Video (FLV) codec. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2987	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable integer overflow vulnerability related to Flash Broker COM. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2988	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability when performing garbage collection. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2990	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability in the h264 decompression routine. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2991	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability in the h264 codec (related to decompression). Successful exploitation could lead to arbitrary code execution.
CVE-2017-2992	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable heap overflow vulnerability when parsing an MP4 header. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2993	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability related to event handlers. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2994	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable use after free vulnerability in Primetime SDK event dispatch. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2995	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable type confusion vulnerability related to the MessageChannel class. Successful exploitation could lead to arbitrary code execution.

CVE-2017-2996	Adobe Flash Player versions 24.0.0.194 and earlier have an exploitable memory corruption vulnerability in Primetime SDK. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2997	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable buffer overflow / underflow vulnerability in the Primetime TVSDK that supports customizing ad information. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2998	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable memory corruption vulnerability in the Primetime TVSDK API functionality related to timeline interactions. Successful exploitation could lead to arbitrary code execution.
CVE-2017-2999	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable memory corruption vulnerability in the Primetime TVSDK functionality related to hosting playback surface. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3000	Adobe Flash Player versions 24.0.0.221 and earlier have a vulnerability in the random number generator used for constant blinding. Successful exploitation could lead to information disclosure.
CVE-2017-3001	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability related to garbage collection in the ActionScript 2 VM. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3002	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability in the ActionScript2 TextField object related to the variable property. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3003	Adobe Flash Player versions 24.0.0.221 and earlier have an exploitable use after free vulnerability related to an interaction between the privacy user interface and the ActionScript 2 Camera object. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3058	Adobe Flash Player versions 25.0.0.127 and earlier have an exploitable use after free vulnerability in the sound class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3059	Adobe Flash Player versions 25.0.0.127 and earlier have an exploitable use after free vulnerability in the internal script object. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3060	Adobe Flash Player versions 25.0.0.127 and earlier have an exploitable memory corruption vulnerability in the ActionScript2 code parser. Successful exploitation could lead to arbitrary code execution.

CVE-2017-3061	Adobe Flash Player versions 25.0.0.127 and earlier have an exploitable memory corruption vulnerability in the SWF parser. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3062	Adobe Flash Player versions 25.0.0.127 and earlier have an exploitable use after free vulnerability in ActionScript2 when creating a getter/setter property. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3063	Adobe Flash Player versions 25.0.0.127 and earlier have an exploitable use after free vulnerability in the ActionScript2 NetStream class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3064	Adobe Flash Player versions 25.0.0.127 and earlier have an exploitable memory corruption vulnerability when parsing a shape outline. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3068	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable memory corruption vulnerability in the Advanced Video Coding engine. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3069	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable memory corruption vulnerability in the BlendMode class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3070	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable memory corruption vulnerability in the ConvolutionFilter class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3071	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable use after free vulnerability when masking display objects. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3072	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable memory corruption vulnerability in the BitmapData class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3073	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable use after free vulnerability when handling multiple mask properties of display objects, aka memory corruption. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3074	Adobe Flash Player versions 25.0.0.148 and earlier have an exploitable memory corruption vulnerability in the Graphics class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3075	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability when

	manipulating the ActionsScript 2 XML class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3076	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the MPEG-4 AVC module. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3077	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the PNG image parser. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3078	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the Adobe Texture Format (ATF) module. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3079	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the internal representation of raster data. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3080	Adobe Flash Player versions 26.0.0.131 and earlier have a security bypass vulnerability related to the Flash API used by Internet Explorer. Successful exploitation could lead to information disclosure.
CVE-2017-3081	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability during internal computation caused by multiple display object mask manipulations. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3082	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable memory corruption vulnerability in the LocaleID class. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3083	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability in the Primetime SDK functionality related to the profile metadata of the media stream. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3084	Adobe Flash Player versions 25.0.0.171 and earlier have an exploitable use after free vulnerability in the advertising metadata functionality. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3085	Adobe Flash Player versions 26.0.0.137 and earlier have a security bypass vulnerability that leads to information disclosure when performing URL redirect.
CVE-2017-3099	Adobe Flash Player versions 26.0.0.131 and earlier have an exploitable memory corruption vulnerability in the Action Script 3 raster data model. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3100	Adobe Flash Player versions 26.0.0.131 and earlier have an exploitable memory corruption vulnerability

	in the Action Script 2 BitmapData class. Successful exploitation could lead to memory address disclosure.
CVE-2017-3106	Adobe Flash Player versions 26.0.0.137 and earlier have an exploitable type confusion vulnerability when parsing SWF files. Successful exploitation could lead to arbitrary code execution.
CVE-2017-3112	An issue was discovered in Adobe Flash Player 27.0.0.183 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is part of AdobePSDK metadata. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure.
CVE-2017-3114	An issue was discovered in Adobe Flash Player 27.0.0.183 and earlier versions. This vulnerability occurs as a result of a computation that reads data that is past the end of the target buffer; the computation is part of providing language- and region- or country-specific functionality. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure.
CVE-2017-5006	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled object owner relationships, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-5007	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled the sequence of events when closing a page, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-5008	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed attacker controlled JavaScript to be run during the invocation of a private script method, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-5009	WebRTC in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5010	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, resolved promises in an inappropriate context, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.

CVE-2017-5011	Google Chrome prior to 56.0.2924.76 for Windows insufficiently sanitized DevTools URLs, which allowed a remote attacker who convinced a user to install a malicious extension to read filesystem contents via a crafted HTML page.
CVE-2017-5012	A heap buffer overflow in V8 in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5013	Google Chrome prior to 56.0.2924.76 for Linux incorrectly handled new tab page navigations in non-selected tabs, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-5014	Heap buffer overflow during image processing in Skia in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5015	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled Unicode glyphs, which allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5016	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to prevent certain UI elements from being displayed by non-visible pages, which allowed a remote attacker to show certain UI elements on a page they don't control via a crafted HTML page.
CVE-2017-5017	Interactions with the OS in Google Chrome prior to 56.0.2924.76 for Mac insufficiently cleared video memory, which allowed a remote attacker to possibly extract image fragments on systems with GeForce 8600M graphics chips via a crafted HTML page.
CVE-2017-5018	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, had an insufficiently strict content security policy on the Chrome app launcher page, which allowed a remote attacker to inject scripts or HTML into a privileged page via a crafted HTML page.
CVE-2017-5019	A use after free in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5020	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to require a user gesture for powerful download operations, which allowed a remote attacker who

	convinced a user to install a malicious extension to execute arbitrary code via a crafted HTML page.
CVE-2017-5021	A use after free in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5022	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to properly enforce unsafe-inline content security policy, which allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2017-5023	Type confusion in Histogram in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit a near null dereference via a crafted HTML page.
CVE-2017-5024	FFmpeg in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2017-5025	FFmpeg in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2017-5026	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to prevent alerts from being displayed by swapped out frames, which allowed a remote attacker to show alerts on a page they don't control via a crafted HTML page.
CVE-2017-5027	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to properly enforce unsafe-inline content security policy, which allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2017-5029	The xsltAddTextString function in transform.c in libxslt 1.1.29, as used in Blink in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android, lacked a check for integer overflow during a size calculation, which allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2017-5030	Incorrect handling of complex species in V8 in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac and 57.0.2987.108 for Android allowed a remote attacker to execute arbitrary code via a crafted HTML page.

CVE-2017-5031	A use after free in ANGLE in Google Chrome prior to 57.0.2987.98 for Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5032	PDFium in Google Chrome prior to 57.0.2987.98 for Windows could be made to increment off the end of a buffer, which allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-5033	Blink in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android failed to correctly propagate CSP restrictions to local scheme pages, which allowed a remote attacker to bypass content security policy via a crafted HTML page, related to the unsafe-inline keyword.
CVE-2017-5034	A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Linux and Windows allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2017-5035	Google Chrome prior to 57.0.2987.98 for Windows and Mac had a race condition, which could cause Chrome to display incorrect certificate information for a site.
CVE-2017-5036	A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to have an unspecified impact via a crafted PDF file.
CVE-2017-5037	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5038	Chrome Apps in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac had a use after free bug in GuestView, which allowed a remote attacker to perform an out of bounds memory read via a crafted Chrome extension.
CVE-2017-5039	A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-5040	V8 in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android was missing a neutering check, which allowed a remote attacker to read values in memory via a crafted HTML page.
CVE-2017-5041	Google Chrome prior to 57.0.2987.100 incorrectly handled back-forward navigation, which allowed a remote attacker to display incorrect information for a site via a crafted HTML page.

CVE-2017-5042	Cast in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android sent cookies to sites discovered via SSDP, which allowed an attacker on the local network segment to initiate connections to arbitrary URLs and observe any plaintext cookies sent.
CVE-2017-5043	Chrome Apps in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac had a use after free bug in GuestView, which allowed a remote attacker to perform an out of bounds memory read via a crafted Chrome extension.
CVE-2017-5044	Heap buffer overflow in filter processing in Skia in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5045	XSS Auditor in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed detection of a blocked iframe load, which allowed a remote attacker to brute force JavaScript variables via a crafted HTML page.
CVE-2017-5046	V8 in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android had insufficient policy enforcement, which allowed a remote attacker to spoof the location object via a crafted HTML page, related to Blink information disclosure.
CVE-2017-5047	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5048	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5049	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5050	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5051	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker

	to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5052	An incorrect assumption about block structure in Blink in Google Chrome prior to 57.0.2987.133 for Mac, Windows, and Linux, and 57.0.2987.132 for Android, allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page that triggers improper casting.
CVE-2017-5053	An out-of-bounds read in V8 in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page, related to Array.prototype.indexOf.
CVE-2017-5054	An out-of-bounds read in V8 in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker to obtain heap memory contents via a crafted HTML page.
CVE-2017-5055	A use after free in printing in Google Chrome prior to 57.0.2987.133 for Linux and Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5056	A use after free in Blink in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5057	Type confusion in PDFium in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2017-5058	A use after free in PrintPreview in Google Chrome prior to 58.0.3029.81 for Windows allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2017-5059	Type confusion in Blink in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac, and 58.0.3029.83 for Android, allowed a remote attacker to potentially obtain code execution via a crafted HTML page.
CVE-2017-5060	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5061	A race condition in navigation in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.

CVE-2017-5062	A use after free in Chrome Apps in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to potentially perform out of bounds memory access via a crafted Chrome extension.
CVE-2017-5063	A numeric overflow in Skia in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac, and 58.0.3029.83 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5064	Incorrect handling of DOM changes in Blink in Google Chrome prior to 58.0.3029.81 for Windows allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5065	Lack of an appropriate action on page navigation in Blink in Google Chrome prior to 58.0.3029.81 for Windows and Mac allowed a remote attacker to potentially confuse a user into making an incorrect security decision via a crafted HTML page.
CVE-2017-5066	Insufficient consistency checks in signature handling in the networking stack in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to incorrectly accept a badly formed X.509 certificate via a crafted HTML page.
CVE-2017-5067	An insufficient watchdog timer in navigation in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-5068	Incorrect handling of picture ID in WebRTC in Google Chrome prior to 58.0.3029.96 for Mac, Windows, and Linux allowed a remote attacker to trigger a race condition via a crafted HTML page.
CVE-2017-5069	Incorrect MIME type of XSS-Protection reports in Blink in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac, and 58.0.3029.83 for Android, allowed a remote attacker to circumvent Cross-Origin Resource Sharing checks via a crafted HTML page.
CVE-2017-5070	Type confusion in V8 in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2017-5071	Insufficient validation of untrusted input in V8 in Google Chrome prior to 59.0.3071.86 for Linux, Windows and Mac, and 59.0.3071.92 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.

CVE-2017-5072	Inappropriate implementation in Omnibox in Google Chrome prior to 59.0.3071.92 for Android allowed a remote attacker to perform domain spoofing with RTL characters via a crafted URL page.
CVE-2017-5073	Use after free in print preview in Blink in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5074	A use after free in Chrome Apps in Google Chrome prior to 59.0.3071.86 for Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page, related to Bluetooth.
CVE-2017-5075	Inappropriate implementation in CSP reporting in Blink in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to obtain the value of url fragments via a crafted HTML page.
CVE-2017-5076	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5077	Insufficient validation of untrusted input in Skia in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5078	Insufficient validation of untrusted input in Blink's mailto: handling in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac allowed a remote attacker to perform command injection via a crafted HTML page, a similar issue to CVE-2004-0121. For example, characters such as * have an incorrect interaction with xdg-email in xdg-utils, and a space character can be used in front of a command-line argument.
CVE-2017-5079	Inappropriate implementation in Blink in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed a remote attacker to display UI on a non attacker controlled tab via a crafted HTML page.
CVE-2017-5080	A use after free in credit card autofill in Google Chrome prior to 59.0.3071.86 for Linux and Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5081	Lack of verification of an extension's locale folder in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android,

	allowed an attacker with local write access to modify extensions by modifying extension files.
CVE-2017-5082	Failure to take advantage of available mitigations in credit card autofill in Google Chrome prior to 59.0.3071.92 for Android allowed a local attacker to take screen shots of credit card information via a crafted HTML page.
CVE-2017-5083	Inappropriate implementation in Blink in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed a remote attacker to display UI on a non attacker controlled tab via a crafted HTML page.
CVE-2017-5085	Inappropriate implementation in Bookmarks in Google Chrome prior to 59 for iOS allowed a remote attacker who convinced the user to perform certain operations to run JavaScript on chrome:// pages via a crafted bookmark.
CVE-2017-5086	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 59.0.3071.86 for Windows and Mac allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5087	A use after free in Blink in Google Chrome prior to 59.0.3071.104 for Mac, Windows, and Linux, and 59.0.3071.117 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page, aka an IndexedDB sandbox escape.
CVE-2017-5088	Insufficient validation of untrusted input in V8 in Google Chrome prior to 59.0.3071.104 for Mac, Windows, and Linux, and 59.0.3071.117 for Android, allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.
CVE-2017-5089	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 59.0.3071.104 for Mac allowed a remote attacker to perform domain spoofing via a crafted domain name.
CVE-2017-5091	A use after free in IndexedDB in Google Chrome prior to 60.0.3112.78 for Linux, Android, Windows, and Mac allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5092	Insufficient validation of untrusted input in PPAPI Plugins in Google Chrome prior to 60.0.3112.78 for Windows allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2017-5093	Inappropriate implementation in modal dialog handling in Blink in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to prevent a full screen warning from being displayed via a crafted HTML page.

CVE-2017-5094	Type confusion in extensions JavaScript bindings in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to potentially maliciously modify objects via a crafted HTML page.
CVE-2017-5095	Stack overflow in PDFium in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to potentially exploit stack corruption via a crafted PDF file.
CVE-2017-5097	Insufficient validation of untrusted input in Skia in Google Chrome prior to 60.0.3112.78 for Linux allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5098	A use after free in V8 in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5099	Insufficient validation of untrusted input in PPAPI Plugins in Google Chrome prior to 60.0.3112.78 for Mac allowed a remote attacker to potentially gain privilege elevation via a crafted HTML page.
CVE-2017-5100	A use after free in Apps in Google Chrome prior to 60.0.3112.78 for Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5101	Inappropriate implementation in Omnibox in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to spoof the contents of the Omnibox via a crafted HTML page.
CVE-2017-5102	Use of an uninitialized value in Skia in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5103	Use of an uninitialized value in Skia in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5104	Inappropriate implementation in interstitials in Google Chrome prior to 60.0.3112.78 for Mac allowed a remote attacker to spoof the contents of the omnibox via a crafted HTML page.
CVE-2017-5105	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.

CVE-2017-5106	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5107	A timing attack in SVG rendering in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to extract pixel values from a cross-origin page being iframe'd via a crafted HTML page.
CVE-2017-5108	Type confusion in PDFium in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to potentially maliciously modify objects via a crafted PDF file.
CVE-2017-5109	Inappropriate implementation of unload handler handling in permission prompts in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to display UI on a non attacker controlled tab via a crafted HTML page.
CVE-2017-5110	Inappropriate implementation of the web payments API on blob: and data: schemes in Web Payments in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to spoof the contents of the Omnibox via a crafted HTML page.
CVE-2017-5111	A use after free in PDFium in Google Chrome prior to 61.0.3163.79 for Linux, Windows, and Mac allowed a remote attacker to potentially exploit memory corruption via a crafted PDF file.
CVE-2017-5112	Heap buffer overflow in WebGL in Google Chrome prior to 61.0.3163.79 for Windows allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2017-5113	Math overflow in Skia in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5114	Inappropriate use of partition alloc in PDFium in Google Chrome prior to 61.0.3163.79 for Linux, Windows, and Mac, and 61.0.3163.81 for Android, allowed a remote attacker to potentially exploit memory corruption via a crafted PDF file.
CVE-2017-5115	Type confusion in V8 in Google Chrome prior to 61.0.3163.79 for Windows allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2017-5116	Type confusion in V8 in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and

	61.0.3163.81 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2017-5117	Use of an uninitialized value in Skia in Google Chrome prior to 61.0.3163.79 for Linux and Windows allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5118	Blink in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, failed to correctly propagate CSP restrictions to javascript scheme pages, which allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2017-5119	Use of an uninitialized value in Skia in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5120	Inappropriate use of www mismatch redirects in browser navigation in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to potentially downgrade HTTPS requests to HTTP via a crafted HTML page. In other words, Chrome could transmit cleartext even though the user had entered an https URL, because of a misdesigned workaround for cases where the domain name in a URL almost matches the domain name in an X.509 server certificate (but differs in the initial "www." substring).
CVE-2017-5121	Inappropriate use of JIT optimisation in V8 in Google Chrome prior to 61.0.3163.100 for Linux, Windows, and Mac allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page, related to the escape analysis phase.
CVE-2017-5122	Inappropriate use of table size handling in V8 in Google Chrome prior to 61.0.3163.100 for Windows allowed a remote attacker to trigger out-of-bounds access via a crafted HTML page.
CVE-2017-5124	Incorrect application of sandboxing in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted MHTML page.
CVE-2017-5125	Heap buffer overflow in Skia in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5126	A use after free in PDFium in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.

CVE-2017-5127	Use after free in PDFium in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-5128	Heap buffer overflow in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, related to WebGL.
CVE-2017-5129	A use after free in WebAudio in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5130	An integer overflow in xmlmemory.c in libxml2 before 2.9.5, as used in Google Chrome prior to 62.0.3202.62 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted XML file.
CVE-2017-5131	An integer overflow in Skia in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka an out-of-bounds write.
CVE-2017-5132	Inappropriate implementation in V8 in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka incorrect WebAssembly stack manipulation.
CVE-2017-5133	Off-by-one read/write on the heap in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to corrupt memory and possibly leak information and potentiality execute code via a crafted PDF file.
CVE-2017-5715	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
CVE-2017-5934	Cross-site scripting (XSS) vulnerability in the link dialogue in GUI editor in MoinMoin before 1.9.10 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2017-7000	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. macOS before 10.12.5 is affected. The issue involves the "SQLite" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7810	Memory safety bugs were reported in Firefox 55 and Firefox ESR 52.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 56, Firefox ESR < 52.4, and Thunderbird < 52.4.
CVE-2017-7826	Memory safety bugs were reported in Firefox 56 and Firefox ESR 52.4. Some of these bugs showed

	evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 57, Firefox ESR < 52.5, and Thunderbird < 52.5.
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-2018-0360	ClamAV before 0.100.1 has an HWP integer overflow with a resultant infinite loop via a crafted Hangul Word Processor file. This is in parsehwp3_paragraph() in libclamav/hwp.c.
CVE-2018-0361	ClamAV before 0.100.1 lacks a PDF object length check, resulting in an unreasonably long time to parse a relatively small file.
CVE-2018-0494	GNU Wget before 1.19.5 is prone to a cookie injection vulnerability in the resp_new function in http.c via a \r\n sequence in a continuation line.
CVE-2018-0495	Libgcrypt before 1.7.10 and 1.8.x before 1.8.3 allows a memory-cache side-channel attack on ECDSA signatures that can be mitigated through the use of blinding during the signing process in the _gcry_ecc_ecdsa_sign function in cipher/ecc-ecdsa.c, aka the Return Of the Hidden Number Problem or ROHNP. To discover an ECDSA key, the attacker needs access to either the local machine or a different virtual machine on the same physical host.
CVE-2018-0499	A cross-site scripting vulnerability in queryparser/ termgenerator_internal.cc in Xapian xapian-core before 1.4.6 exists due to incomplete HTML escaping by Xapian::MSet::snippet().
CVE-2018-0500	Curl_smtp_escape_eob in lib/smtp.c in curl 7.54.1 to and including curl 7.60.0 has a heap-based buffer overflow that might be exploitable by an attacker who can control the data that curl transmits over SMTP with certain settings (i.e., use of a nonstandard --limit-rate argument or CURLOPT_BUFFERSIZE value).
CVE-2018-0502	An issue was discovered in zsh before 5.6. The beginning of a #! script file was mishandled, potentially leading to an execve call to a program named on the second line.
CVE-2018-0732	During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a

	Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).
CVE-2018-0737	The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).
CVE-2018-1000200	The Linux Kernel versions 4.14, 4.15, and 4.16 has a null pointer dereference which can result in an out of memory (OOM) killing of large mlocked processes. The issue arises from an oom killed process's final thread calling exit_mmap(), which calls munlock_vma_pages_all() for mlocked vmas.This can happen synchronously with the oom reaper's unmap_page_range() since the vma's VM_LOCKED bit is cleared before munlocking (to determine if any other vmas share the memory and are mlocked).
CVE-2018-1000204	** DISPUTED ** Linux Kernel version 3.18 to 4.16 incorrectly handles an SG_IO ioctl on /dev/sg0 with dxfer_direction=SG_DXFER_FROM_DEV and an empty 6-byte cmdp. This may lead to copying up to 1000 kernel heap pages to the userspace. This has been fixed upstream in https://github.com/torvalds/linux/commit/a45b599ad808c3c982fdcdc12b0b8611c2f92824 already. The problem has limited scope, as users don't usually have permissions to access SCSI devices. On the other hand, e.g. the Nero user manual suggests doing `chmod o+r+w /dev/sg*` to make the devices accessible. NOTE: third parties dispute the relevance of this report, noting that the requirement for an attacker to have both the CAP_SYS_ADMIN and CAP_SYS_RAWIO capabilities makes it "virtually impossible to exploit."
CVE-2018-1000222	Libgd version 2.2.5 contains a Double Free Vulnerability vulnerability in gdImageBmpPtr Function that can result in Remote Code Execution . This attack appear to be exploitable via Specially Crafted Jpeg Image can trigger double free. This vulnerability appears to have been fixed in after commit ac16bdf2d41724b5a65255d4c28fb0ec46bc42f5.
CVE-2018-1000300	curl version curl 7.54.1 to and including curl 7.59.0 contains a CWE-122: Heap-based Buffer Overflow vulnerability in denial of service and more that can result in curl might overflow a heap based memory buffer when closing down an FTP connection with very long server command replies.. This vulnerability

	appears to have been fixed in curl < 7.54.1 and curl >= 7.60.0.
CVE-2018-1000301	curl version curl 7.20.0 to and including curl 7.59.0 contains a CWE-126: Buffer Over-read vulnerability in denial of service that can result in curl can be tricked into reading data beyond the end of a heap based buffer used to store downloaded RTSP content.. This vulnerability appears to have been fixed in curl < 7.20.0 and curl >= 7.60.0.
CVE-2018-1000802	Python Software Foundation Python (CPython) version 2.7 contains a CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in shutil module (make_archive function) that can result in Denial of service, Information gain via injection of arbitrary files on the system or entire drive. This attack appear to be exploitable via Passage of unfiltered user input to the function. This vulnerability appears to have been fixed in after commit add531a1e55b0a739b0f42582f1c9747e5649ace.
CVE-2018-1000805	Paramiko version 2.4.1, 2.3.2, 2.2.3, 2.1.5, 2.0.8, 1.18.5, 1.17.6 contains a Incorrect Access Control vulnerability in SSH server that can result in RCE. This attack appear to be exploitable via network connectivity.
CVE-2018-10021	** DISPUTED ** drivers/scsi/libsas/sas_scsi_host.c in the Linux kernel before 4.16 allows local users to cause a denial of service (ata qc leak) by triggering certain failure conditions. NOTE: a third party disputes the relevance of this report because the failure can only occur for physically proximate attackers who unplug SAS Host Bus Adapter cables.
CVE-2018-10177	In ImageMagick 7.0.7-28, there is an infinite loop in the ReadOneMNGImage function of the coders/png.c file. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted mng file.
CVE-2018-10194	The set_text_distance function in devices/vector/gdevpdts.c in the pdfwrite component in Artifex Ghostscript through 9.22 does not prevent overflows in text-positioning calculation, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PDF document.
CVE-2018-10196	NULL pointer dereference vulnerability in the rebuild_vlists function in lib/dotgen/conc.c in the dotgen library in Graphviz 2.40.1 allows remote attackers to cause a denial of service (application crash) via a crafted file.
CVE-2018-10323	The xfs_bmap_extents_to_btree function in fs/xfs/libxfs/xfs_bmap.c in the Linux kernel through 4.16.3 allows local users to cause a denial of service

	(xfs_bmapi_write NULL pointer dereference) via a crafted xfs image.
CVE-2018-10360	The do_core_note function in readelf.c in libmagic.a in file 5.33 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted ELF file.
CVE-2018-10528	An issue was discovered in LibRaw 0.18.9. There is a stack-based buffer overflow in the utf2char function in libraw_cxx.cpp.
CVE-2018-10529	An issue was discovered in LibRaw 0.18.9. There is an out-of-bounds read affecting the X3F property table list implementation in libraw_x3f.cpp and libraw_cxx.cpp.
CVE-2018-10536	An issue was discovered in WavPack 5.1.0 and earlier. The WAV parser component contains a vulnerability that allows writing to memory because ParseRiffHeaderConfig in riff.c does not reject multiple format chunks.
CVE-2018-10537	An issue was discovered in WavPack 5.1.0 and earlier. The W64 parser component contains a vulnerability that allows writing to memory because ParseWave64HeaderConfig in wave64.c does not reject multiple format chunks.
CVE-2018-10538	An issue was discovered in WavPack 5.1.0 and earlier for WAV input. Out-of-bounds writes can occur because ParseRiffHeaderConfig in riff.c does not validate the sizes of unknown chunks before attempting memory allocation, related to a lack of integer-overflow protection within a bytes_to_copy calculation and subsequent malloc call, leading to insufficient memory allocation.
CVE-2018-10539	An issue was discovered in WavPack 5.1.0 and earlier for DSDiff input. Out-of-bounds writes can occur because ParseDsdiffHeaderConfig in dsdiff.c does not validate the sizes of unknown chunks before attempting memory allocation, related to a lack of integer-overflow protection within a bytes_to_copy calculation and subsequent malloc call, leading to insufficient memory allocation.
CVE-2018-10540	An issue was discovered in WavPack 5.1.0 and earlier for W64 input. Out-of-bounds writes can occur because ParseWave64HeaderConfig in wave64.c does not validate the sizes of unknown chunks before attempting memory allocation, related to a lack of integer-overflow protection within a bytes_to_copy calculation and subsequent malloc call, leading to insufficient memory allocation.
CVE-2018-10545	An issue was discovered in PHP before 5.6.35, 7.0.x before 7.0.29, 7.1.x before 7.1.16, and 7.2.x before 7.2.4. Dumpable FPM child processes allow bypassing opcache access controls because fpm_unix.c makes a

	PR_SET_DUMPABLE prctl call, allowing one user (in a multiuser environment) to obtain sensitive information from the process memory of a second user's PHP applications by running gcore on the PID of the PHP-FPM worker process.
CVE-2018-10546	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. An infinite loop exists in ext/iconv/iconv.c because the iconv stream filter does not reject invalid multibyte sequences.
CVE-2018-10547	An issue was discovered in ext/phar/phar_object.c in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. There is Reflected XSS on the PHAR 403 and 404 error pages via request data of a request for a .phar file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2018-5712.
CVE-2018-10548	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. ext/ldap/ldap.c allows remote LDAP servers to cause a denial of service (NULL pointer dereference and application crash) because of mishandling of the ldap_get_dn return value.
CVE-2018-10549	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_iif_add_value mishandles the case of a MakerNote that lacks a final '\0' character.
CVE-2018-1059	The DPDK vhost-user interface does not check to verify that all the requested guest physical range is mapped and contiguous when performing Guest Physical Addresses to Host Virtual Addresses translations. This may lead to a malicious guest exposing vhost-user backend process memory. All versions before 18.02.1 are vulnerable.
CVE-2018-1064	libvirt version before 4.2.0-rc1 is vulnerable to a resource exhaustion as a result of an incomplete fix for CVE-2018-5748 that affects QEMU monitor but now also triggered via QEMU guest agent.
CVE-2018-10768	There is a NULL pointer dereference in the AnnotPath::getCoordsLength function in Annot.h in an Ubuntu package for Poppler 0.24.5. A crafted input will lead to a remote denial of service attack. Later Ubuntu packages such as for Poppler 0.41.0 are not affected.
CVE-2018-10804	ImageMagick version 7.0.7-28 contains a memory leak in WriteTIFFImage in coders/tiff.c.
CVE-2018-10805	ImageMagick version 7.0.7-28 contains a memory leak in ReadYCBCRImage in coders/ycbcr.c.

CVE-2018-10811	strongSwan 5.6.0 and older allows Remote Denial of Service because of Missing Initialization of a Variable.
CVE-2018-10839	Qemu emulator <= 3.0.0 built with the NE2000 NIC emulation support is vulnerable to an integer overflow, which could lead to buffer overflow issue. It could occur when receiving packets over the network. A user inside guest could use this flaw to crash the Qemu process resulting in DoS.
CVE-2018-10840	Linux kernel is vulnerable to a heap-based buffer overflow in the fs/ext4/xattr.c:ext4_xattr_set_entry() function. An attacker could exploit this by operating on a mounted crafted ext4 image.
CVE-2018-10858	A heap-buffer overflow was found in the way samba clients processed extra long filename in a directory listing. A malicious samba server could use this flaw to cause arbitrary code execution on a samba client. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.
CVE-2018-10860	perl-archive-zip is vulnerable to a directory traversal in Archive::Zip. It was found that the Archive::Zip module did not properly sanitize paths while extracting zip files. An attacker able to provide a specially crafted archive for processing could use this flaw to write or overwrite arbitrary files in the context of the perl interpreter.
CVE-2018-10881	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bound access in ext4_get_group_info function, a denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.
CVE-2018-10903	A flaw was found in python-cryptography versions between >=1.9.0 and <2.3. The finalize_with_tag API did not enforce a minimum tag length. If a user did not validate the input length prior to passing it to finalize_with_tag an attacker could craft an invalid payload with a shortened tag (e.g. 1 byte) such that they would have a 1 in 256 chance of passing the MAC check. GCM tag forgeries can cause key leakage.
CVE-2018-10915	A vulnerability was found in libpq, the default PostgreSQL client library where libpq failed to properly reset its internal state between connections. If an affected version of libpq was used with "host" or "hostaddr" connection parameters from untrusted input, attackers could bypass client-side connection security features, obtain access to higher privileged connections or potentially cause other impact through SQL injection, by causing the PQescape() functions to malfunction. Postgresql versions before 10.5, 9.6.10, 9.5.14, 9.4.19, and 9.3.24 are affected.
CVE-2018-10918	A null pointer dereference flaw was found in the way samba checked database outputs from the LDB

	database layer. An authenticated attacker could use this flaw to crash a samba server in an Active Directory Domain Controller configuration. Samba versions before 4.7.9 and 4.8.4 are vulnerable.
CVE-2018-10919	The Samba Active Directory LDAP server was vulnerable to an information disclosure flaw because of missing access control checks. An authenticated attacker could use this flaw to extract confidential attribute values using LDAP search expressions. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.
CVE-2018-1092	The ext4_iget function in fs/ext4/inode.c in the Linux kernel through 4.15.15 mishandles the case of a root directory with a zero i_links_count, which allows attackers to cause a denial of service (ext4_process_freed_data NULL pointer dereference and OOPS) via a crafted ext4 image.
CVE-2018-10925	It was discovered that PostgreSQL versions before 10.5, 9.6.10, 9.5.14, 9.4.19, and 9.3.24 failed to properly check authorization on certain statements involved with "INSERT ... ON CONFLICT DO UPDATE". An attacker with "CREATE TABLE" privileges could exploit this to read arbitrary bytes server memory. If the attacker also had certain "INSERT" and limited "UPDATE" privileges to a particular table, they could exploit this to update other columns in the same table.
CVE-2018-1093	The ext4_valid_block_bitmap function in fs/ext4/balloc.c in the Linux kernel through 4.15.15 allows attackers to cause a denial of service (out-of-bounds read and system crash) via a crafted ext4 image because balloc.c and ialloc.c do not validate bitmap block numbers.
CVE-2018-10933	A vulnerability was found in libssh's server-side state machine before versions 0.7.6 and 0.8.4. A malicious client could create channels without first performing authentication, resulting in unauthorized access.
CVE-2018-1094	The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.15.15 does not always initialize the crc32c checksum driver, which allows attackers to cause a denial of service (ext4_xattr_inode_hash NULL pointer dereference and system crash) via a crafted ext4 image.
CVE-2018-10940	The cdrom_ioctl_media_changed function in drivers/cdrom/cdrom.c in the Linux kernel before 4.16.6 allows local attackers to use a incorrect bounds check in the CDROM driver CDROM_MEDIA_CHANGED ioctl to read out kernel memory.
CVE-2018-1095	The ext4_xattr_check_entries function in fs/ext4/xattr.c in the Linux kernel through 4.15.15 does not properly

	validate xattr sizes, which causes misinterpretation of a size as an error code, and consequently allows attackers to cause a denial of service (get_acl NULL pointer dereference and system crash) via a crafted ext4 image.
CVE-2018-10958	In types.cpp in Exiv2 0.26, a large size value may lead to a SIGABRT during an attempt at memory allocation for an Exiv2::Internal::PngChunk::zlibUncompress call.
CVE-2018-10998	An issue was discovered in Exiv2 0.26. readMetadata in jp2image.cpp allows remote attackers to cause a denial of service (SIGABRT) by triggering an incorrect Safe::add call.
CVE-2018-10999	An issue was discovered in Exiv2 0.26. The Exiv2::Internal::PngChunk::parseTXTChunk function has a heap-based buffer over-read.
CVE-2018-1100	zsh through version 5.4.2 is vulnerable to a stack-based buffer overflow in the utils.c:checkmailpath function. A local attacker could exploit this to execute arbitrary code in the context of another user.
CVE-2018-1108	kernel drivers before version 4.17-rc1 are vulnerable to a weakness in the Linux kernel's implementation of random seed data. Programs, early in the boot sequence, could use the data allocated for the seed before it was sufficiently generated.
CVE-2018-1116	A flaw was found in polkit before version 0.116. The implementation of the polkit_backend_interactive_authority_check_authorization function in polkitd allows to test for authentication and trigger authentication of unrelated processes owned by other users. This may result in a local DoS and information disclosure.
CVE-2018-1118	Linux kernel vhost since version 4.8 does not properly initialize memory in messages passed between virtual guests and the host operating system in the vhost/vhost.c:vhost_new_msg() function. This can allow local privileged users to read some kernel memory contents when reading from the /dev/vhost-net device file.
CVE-2018-1120	A flaw was found affecting the Linux kernel before version 4.17. By mmap()ing a FUSE-backed file onto a process's memory containing command line arguments (or environment strings), an attacker can cause utilities from psutils or procps (such as ps, w) or any other program which makes a read() call to the /proc/<pid>/cmdline (or /proc/<pid>/environ) files to block indefinitely (denial of service) or for some controlled time (as a synchronization primitive for other attacks).
CVE-2018-11212	An issue was discovered in libjpeg 9a. The alloc_sarray function in jmemmgr.c allows remote attackers to cause

	a denial of service (divide-by-zero error) via a crafted file.
CVE-2018-11213	An issue was discovered in libjpeg 9a. The get_text_gray_row function in rdppm.c allows remote attackers to cause a denial of service (Segmentation fault) via a crafted file.
CVE-2018-11214	An issue was discovered in libjpeg 9a. The get_text_rgb_row function in rdppm.c allows remote attackers to cause a denial of service (Segmentation fault) via a crafted file.
CVE-2018-1122	procps-ng before version 3.3.15 is vulnerable to a local privilege escalation in top. If a user runs top with HOME unset in an attacker-controlled directory, the attacker could achieve privilege escalation by exploiting one of several vulnerabilities in the config_file() function.
CVE-2018-1123	procps-ng before version 3.3.15 is vulnerable to a denial of service in ps via mmap buffer overflow. Inbuilt protection in ps maps a guard page at the end of the overflowed buffer, ensuring that the impact of this flaw is limited to a crash (temporary denial of service).
CVE-2018-11233	In Git before 2.13.7, 2.14.x before 2.14.4, 2.15.x before 2.15.2, 2.16.x before 2.16.4, and 2.17.x before 2.17.1, code to sanity-check pathnames on NTFS can result in reading out-of-bounds memory.
CVE-2018-11235	In Git before 2.13.7, 2.14.x before 2.14.4, 2.15.x before 2.15.2, 2.16.x before 2.16.4, and 2.17.x before 2.17.1, remote code execution can occur. With a crafted .gitmodules file, a malicious project can execute an arbitrary script on a machine that runs "git clone --recurse-submodules" because submodule "names" are obtained from this file, and then appended to $GIT_DIR/modules, leading to directory traversal with "../" in a name. Finally, post-checkout hooks from a submodule are executed, bypassing the intended design in which hooks are not obtained from a remote server.
CVE-2018-1124	procps-ng before version 3.3.15 is vulnerable to multiple integer overflows leading to a heap corruption in file2strvec function. This allows a privilege escalation for a local attacker who can create entries in procfs by starting processes, which could result in crashes or arbitrary code execution in proc utilities run by other users.
CVE-2018-1125	procps-ng before version 3.3.15 is vulnerable to a stack buffer overflow in pgrep. This vulnerability is mitigated by FORTIFY, as it involves strncat() to a stack-allocated string. When pgrep is compiled with FORTIFY (as on Red Hat Enterprise Linux and Fedora), the impact is limited to a crash.

CVE-2018-11251	In ImageMagick 7.0.7-23 Q16 x86_64 2018-01-24, there is a heap-based buffer over-read in ReadSUNImage in coders/sun.c, which allows attackers to cause a denial of service (application crash in SetGrayscaleImage in MagickCore/quantize.c) via a crafted SUN image file.
CVE-2018-1126	procps-ng before version 3.3.15 is vulnerable to an incorrect integer size in proc/alloc.* leading to truncation/integer overflow issues. This flaw is related to CVE-2018-1124.
CVE-2018-1139	A flaw was found in the way samba before 4.7.9 and 4.8.4 allowed the use of weak NTLMv1 authentication even when NTLMv1 was explicitly disabled. A man-in-the-middle attacker could use this flaw to read the credential and other details passed between the samba server and client.
CVE-2018-11410	An issue was discovered in Liblouis 3.5.0. A invalid free in the compileRule function in compileTranslationTable.c allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact.
CVE-2018-11412	In the Linux kernel 4.13 through 4.16.11, ext4_read_inline_data() in fs/ext4/inline.c performs a memcpy with an untrusted length value in certain circumstances involving a crafted filesystem that stores the system.data extended attribute value in a dedicated inode.
CVE-2018-11440	Liblouis 3.5.0 has a stack-based Buffer Overflow in the function parseChars in compileTranslationTable.c.
CVE-2018-11469	Incorrect caching of responses to requests including an Authorization header in HAProxy 1.8.0 through 1.8.9 (if cache enabled) allows attackers to achieve information disclosure via an unauthenticated remote request, related to the proto_http.c check_request_for_cacheability function.
CVE-2018-11506	The sr_do_ioctl function in drivers/scsi/sr_ioctl.c in the Linux kernel through 4.16.12 allows local users to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact because sense buffers have different sizes at the CDROM layer and the SCSI layer, as demonstrated by a CDROMREADMODE2 ioctl call.
CVE-2018-11508	The compat_get_timex function in kernel/compat.c in the Linux kernel before 4.16.9 allows local users to obtain sensitive information from kernel memory via adjtimex.
CVE-2018-1152	libjpeg-turbo 1.5.90 is vulnerable to a denial of service vulnerability caused by a divide by zero when processing a crafted BMP image.

CVE-2018-11531	Exiv2 0.26 has a heap-based buffer overflow in getData in preview.cpp.
CVE-2018-11574	Improper input validation together with an integer overflow in the EAP-TLS protocol implementation in PPPD may cause a crash, information disclosure, or authentication bypass. This implementation is distributed as a patch for PPPD 0.91, and includes the affected eap.c and eap-tls.c files. Configurations that use the `refuse-app` option are unaffected.
CVE-2018-11577	Liblouis 3.5.0 has a Segmentation fault in lou_logPrint in logging.c.
CVE-2018-11625	In ImageMagick 7.0.7-37 Q16, SetGrayscaleImage in the quantize.c file allows attackers to cause a heap-based buffer over-read via a crafted file.
CVE-2018-11645	psi/zfile.c in Artifex Ghostscript before 9.21rc1 permits the status command even if -dSAFER is used, which might allow remote attackers to determine the existence and size of arbitrary files, a similar issue to CVE-2016-7977.
CVE-2018-11655	In ImageMagick 7.0.7-20 Q16 x86_64, a memory leak vulnerability was found in the function GetImagePixelCache in MagickCore/cache.c, which allows attackers to cause a denial of service via a crafted CALS image file.
CVE-2018-11656	In ImageMagick 7.0.7-20 Q16 x86_64, a memory leak vulnerability was found in the function ReadDCMImage in coders/dcm.c, which allows attackers to cause a denial of service via a crafted DCM image file.
CVE-2018-11683	Liblouis 3.5.0 has a stack-based Buffer Overflow in the function parseChars in compileTranslationTable.c, a different vulnerability than CVE-2018-11440.
CVE-2018-11684	Liblouis 3.5.0 has a stack-based Buffer Overflow in the function includeFile in compileTranslationTable.c.
CVE-2018-11685	Liblouis 3.5.0 has a stack-based Buffer Overflow in the function compileHyphenation in compileTranslationTable.c.
CVE-2018-11763	In Apache HTTP Server 2.4.17 to 2.4.34, by sending continuous, large SETTINGS frames a client can occupy a connection, server thread and CPU time without any connection timeout coming to effect. This affects only HTTP/2 connections. A possible mitigation is to not enable the h2 protocol.
CVE-2018-11780	A potential Remote Code Execution bug exists with the PDFInfo plugin in Apache SpamAssassin before 3.4.2.
CVE-2018-11781	Apache SpamAssassin 3.4.2 fixes a local user code injection in the meta rule syntax.
CVE-2018-11806	m_cat in slirp/mbuf.c in Qemu has a heap-based buffer overflow via incoming fragmented datagrams.

CVE-2018-12015	In Perl through 5.26.2, the Archive::Tar module allows remote attackers to bypass a directory-traversal protection mechanism, and overwrite arbitrary files, via an archive file containing a symlink and a regular file with the same name.
CVE-2018-12020	mainproc.c in GnuPG before 2.2.8 mishandles the original filename during decryption and verification actions, which allows remote attackers to spoof the output that GnuPG sends on file descriptor 2 to other programs that use the "--status-fd 2" option. For example, the OpenPGP data might represent an original filename that contains line feed characters in conjunction with GOODSIG or VALIDSIG status codes.
CVE-2018-12085	Liblouis 3.6.0 has a stack-based Buffer Overflow in the function parseChars in compileTranslationTable.c, a different vulnerability than CVE-2018-11440.
CVE-2018-12232	In net/socket.c in the Linux kernel through 4.17.1, there is a race condition between fchownat and close in cases where they target the same socket file descriptor, related to the sock_close and sockfs_setattr functions. fchownat does not increment the file descriptor reference count, which allows close to set the socket to NULL during fchownat's execution, leading to a NULL pointer dereference and system crash.
CVE-2018-12233	In the ea_get function in fs/jfs/xattr.c in the Linux kernel through 4.17.1, a memory corruption bug in JFS can be triggered by calling setxattr twice with two different extended attribute names on the same file. This vulnerability can be triggered by an unprivileged user with the ability to create files and execute programs. A kmalloc call is incorrect, leading to slab-out-of-bounds in jfs_xattr.
CVE-2018-12264	Exiv2 0.26 has integer overflows in LoaderTiff::getData() in preview.cpp, leading to an out-of-bounds read in Exiv2::ValueType::setDataArea in value.hpp.
CVE-2018-12265	Exiv2 0.26 has an integer overflow in the LoaderExifJpeg class in preview.cpp, leading to an out-of-bounds read in Exiv2::MemIo::read in basicio.cpp.
CVE-2018-12293	The getImageData function in the ImageBufferCairo class in WebCore/platform/graphics/cairo/ImageBufferCairo.cpp in WebKit, as used in WebKitGTK+ prior to version 2.20.3 and WPE WebKit prior to version 2.20.1, is vulnerable to a heap-based buffer overflow triggered by an integer overflow, which could be abused by crafted HTML content.
CVE-2018-12358	Service workers can use redirection to avoid the tainting of cross-origin resources in some instances, allowing a malicious site to read responses which are supposed to be opaque. This vulnerability affects Firefox < 61.

CVE-2018-12359	A buffer overflow can occur when rendering canvas content while adjusting the height and width of the canvas element dynamically, causing data to be written outside of the currently computed boundaries. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60, Thunderbird < 52.9, Firefox ESR < 60.1, Firefox ESR < 52.9, and Firefox < 61.
CVE-2018-12360	A use-after-free vulnerability can occur when deleting an input element during a mutation event handler triggered by focusing that element. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60, Thunderbird < 52.9, Firefox ESR < 60.1, Firefox ESR < 52.9, and Firefox < 61.
CVE-2018-12361	An integer overflow can occur in the SwizzleData code while calculating buffer sizes. The overflowed value is used for subsequent graphics computations when their inputs are not sanitized which results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60, Firefox ESR < 60.1, and Firefox < 61.
CVE-2018-12362	An integer overflow can occur during graphics operations done by the Supplemental Streaming SIMD Extensions 3 (SSSE3) scaler, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60, Thunderbird < 52.9, Firefox ESR < 60.1, Firefox ESR < 52.9, and Firefox < 61.
CVE-2018-12363	A use-after-free vulnerability can occur when script uses mutation events to move DOM nodes between documents, resulting in the old document that held the node being freed but the node still having a pointer referencing it. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60, Thunderbird < 52.9, Firefox ESR < 60.1, Firefox ESR < 52.9, and Firefox < 61.
CVE-2018-12364	NPAPI plugins, such as Adobe Flash, can send non-simple cross-origin requests, bypassing CORS by making a same-origin POST that does a 307 redirect to the target site. This allows for a malicious site to engage in cross-site request forgery (CSRF) attacks. This vulnerability affects Thunderbird < 60, Thunderbird < 52.9, Firefox ESR < 60.1, Firefox ESR < 52.9, and Firefox < 61.
CVE-2018-12365	A compromised IPC child process can escape the content sandbox and list the names of arbitrary files on the file system without user consent or interaction. This could result in exposure of private local files. This vulnerability affects Thunderbird < 60, Thunderbird < 52.9, Firefox ESR < 60.1, Firefox ESR < 52.9, and Firefox < 61.

CVE-2018-12366	An invalid grid size during QCMS (color profile) transformations can result in the out-of-bounds read interpreted as a float value. This could leak private data into the output. This vulnerability affects Thunderbird < 60, Thunderbird < 52.9, Firefox ESR < 60.1, Firefox ESR < 52.9, and Firefox < 61.
CVE-2018-12367	In the previous mitigations for Spectre, the resolution or precision of various methods was reduced to counteract the ability to measure precise time intervals. In that work PerformanceNavigationTiming was not adjusted but it was found that it could be used as a precision timer. This vulnerability affects Thunderbird < 60, Firefox ESR < 60.1, and Firefox < 61.
CVE-2018-12369	WebExtensions bundled with embedded experiments were not correctly checked for proper authorization. This allowed a malicious WebExtension to gain full browser permissions. This vulnerability affects Firefox ESR < 60.1 and Firefox < 61.
CVE-2018-12370	In Reader View SameSite cookie protections are not checked on exiting. This allows for a payload to be triggered when Reader View is exited if loaded by a malicious site while Reader mode is active, bypassing CSRF protections. This vulnerability affects Firefox < 61.
CVE-2018-12371	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-12372	Decrypted S/MIME parts, when included in HTML crafted for an attack, can leak plaintext when included in a a HTML reply/forward. This vulnerability affects Thunderbird < 52.9.
CVE-2018-12373	dDecrypted S/MIME parts hidden with CSS or the plaintext HTML tag can leak plaintext when included in a HTML reply/forward. This vulnerability affects Thunderbird < 52.9.
CVE-2018-12374	Plaintext of decrypted emails can leak through by user submitting an embedded form by pressing enter key within a text input field. This vulnerability affects Thunderbird < 52.9.
CVE-2018-12375	Memory safety bugs present in Firefox 61. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 62.
CVE-2018-12376	Memory safety bugs present in Firefox 61 and Firefox ESR 60.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run

	arbitrary code. This vulnerability affects Firefox < 62, Firefox ESR < 60.2, and Thunderbird < 60.2.1.
CVE-2018-12377	A use-after-free vulnerability can occur when refresh driver timers are refreshed in some circumstances during shutdown when the timer is deleted while still in use. This results in a potentially exploitable crash. This vulnerability affects Firefox < 62, Firefox ESR < 60.2, and Thunderbird < 60.2.1.
CVE-2018-12378	A use-after-free vulnerability can occur when an IndexedDB index is deleted while still in use by JavaScript code that is providing payload values to be stored. This results in a potentially exploitable crash. This vulnerability affects Firefox < 62, Firefox ESR < 60.2, and Thunderbird < 60.2.1.
CVE-2018-12383	If a user saved passwords before Firefox 58 and then later set a master password, an unencrypted copy of these passwords is still accessible. This is because the older stored password file was not deleted when the data was copied to a new format starting in Firefox 58. The new master password is added only on the new file. This could allow the exposure of stored password data outside of user expectations. This vulnerability affects Firefox < 62, Firefox ESR < 60.2.1, and Thunderbird < 60.2.1.
CVE-2018-12385	A potentially exploitable crash in TransportSecurityInfo used for SSL can be triggered by data stored in the local cache in the user profile directory. This issue is only exploitable in combination with another vulnerability allowing an attacker to write data into the local cache or from locally installed malware. This issue also triggers a non-exploitable startup crash for users switching between the Nightly and Release versions of Firefox if the same profile is used. This vulnerability affects Thunderbird < 60.2.1, Firefox ESR < 60.2.1, and Firefox < 62.0.2.
CVE-2018-12386	A vulnerability in register allocation in JavaScript can lead to type confusion, allowing for an arbitrary read and write. This leads to remote code execution inside the sandboxed content process when triggered. This vulnerability affects Firefox ESR < 60.2.2 and Firefox < 62.0.3.
CVE-2018-12387	A vulnerability where the JavaScript JIT compiler inlines Array.prototype.push with multiple arguments that results in the stack pointer being off by 8 bytes after a bailout. This leaks a memory address to the calling function which can be used as part of an exploit inside the sandboxed content process. This vulnerability affects Firefox ESR < 60.2.2 and Firefox < 62.0.3.
CVE-2018-12390	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the

	candidate has been publicized, the details for this candidate will be provided.
CVE-2018-12392	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-12393	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-12395	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-12396	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-12397	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-12599	In ImageMagick 7.0.8-3 Q16, ReadBMPImage and WriteBMPImage in coders/bmp.c allow attackers to cause an out of bounds write via a crafted file.
CVE-2018-12600	In ImageMagick 7.0.8-3 Q16, ReadDIBImage and WriteDIBImage in coders/dib.c allow attackers to cause an out of bounds write via a crafted file.
CVE-2018-12617	qmp_guest_file_read in qga/commands-posix.c and qga/commands-win32.c in qemu-ga (aka QEMU Guest Agent) in QEMU 2.12.50 has an integer overflow causing a g_malloc0() call to trigger a segmentation fault when trying to allocate a large memory chunk. The vulnerability can be exploited by sending a crafted QMP command (including guest-file-read with a large count value) to the agent via the listening socket.
CVE-2018-12824	Adobe Flash Player 30.0.0.134 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-12825	Adobe Flash Player 30.0.0.134 and earlier have a security bypass vulnerability. Successful exploitation could lead to security mitigation bypass.

CVE-2018-12826	Adobe Flash Player 30.0.0.134 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-12827	Adobe Flash Player 30.0.0.134 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-12828	Adobe Flash Player 30.0.0.134 and earlier have a "use of a component with a known vulnerability" vulnerability. Successful exploitation could lead to privilege escalation.
CVE-2018-1283	In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.
CVE-2018-12882	exif_read_from_impl in ext/exif/exif.c in PHP 7.2.x through 7.2.7 allows attackers to trigger a use-after-free (in exif_read_from_file) because it closes a stream that it is not responsible for closing. The vulnerable code is reachable through the PHP exif_read_data function.
CVE-2018-12904	In arch/x86/kvm/vmx.c in the Linux kernel before 4.17.2, when nested virtualization is used, local attackers could cause L1 KVM guests to VMEXIT, potentially allowing privilege escalations and denial of service attacks due to lack of checking of CPL.
CVE-2018-12910	The get_cookies function in soup-cookie-jar.c in libsoup 2.63.2 allows attackers to have unspecified impact via an empty hostname.
CVE-2018-12911	WebKitGTK+ 2.20.3 has an off-by-one error, with a resultant out-of-bounds write, in the get_simple_globs functions in ThirdParty/xdgmime/src/xdgmimecache.c and ThirdParty/xdgmime/src/xdgmimeglob.c.
CVE-2018-1301	A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.
CVE-2018-1302	When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the

	team could not reproduce it outside debug builds, so it is classified as low risk.
CVE-2018-1303	A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.
CVE-2018-1304	The URL pattern of "" (the empty string) which exactly maps to the context root was not correctly handled in Apache Tomcat 9.0.0.M1 to 9.0.4, 8.5.0 to 8.5.27, 8.0.0.RC1 to 8.0.49 and 7.0.0 to 7.0.84 when used as part of a security constraint definition. This caused the constraint to be ignored. It was, therefore, possible for unauthorised users to gain access to web application resources that should have been protected. Only security constraints with a URL pattern of the empty string were affected.
CVE-2018-13043	scripts/grep-excuses.pl in Debian devscripts through 2.18.3 allows code execution through unsafe YAML loading because YAML::Syck is used without a configuration that prevents unintended blessing.
CVE-2018-1305	Security constraints defined by annotations of Servlets in Apache Tomcat 9.0.0.M1 to 9.0.4, 8.5.0 to 8.5.27, 8.0.0.RC1 to 8.0.49 and 7.0.0 to 7.0.84 were only applied once a Servlet had been loaded. Because security constraints defined in this way apply to the URL pattern and any URLs below that point, it was possible - depending on the order Servlets were loaded - for some security constraints not to be applied. This could have exposed resources to users who were not authorised to access them.
CVE-2018-13094	An issue was discovered in fs/xfs/libxfs/xfs_attr_leaf.c in the Linux kernel through 4.17.3. An OOPS may occur for a corrupted xfs image after xfs_da_shrink_inode() is called with a NULL bp.
CVE-2018-1312	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
CVE-2018-13153	In ImageMagick 7.0.8-4, there is a memory leak in the XMagickCommand function in MagickCore/animate.c.
CVE-2018-13259	An issue was discovered in zsh before 5.6. Shebang lines exceeding 64 characters were truncated,

	potentially leading to an execve call to a program name that is a substring of the intended one.
CVE-2018-1333	By specially crafting HTTP/2 requests, workers would be allocated 60 seconds longer than necessary, leading to worker exhaustion and a denial of service. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.18-2.4.30,2.4.33).
CVE-2018-13405	The inode_init_owner function in fs/inode.c in the Linux kernel through 4.17.4 allows local users to create files with an unintended group ownership, in a scenario where a directory is SGID to a certain group and is writable by a user who is not a member of that group. Here, the non-member can trigger creation of a plain file whose group ownership is that group. The intended behavior was that the non-member can trigger creation of a directory (but not a plain file) whose group ownership is that group. The non-member can escalate privileges by making the plain file executable and SGID.
CVE-2018-13406	An integer overflow in the uvesafb_setcmap function in drivers/video/fbdev/uvesafb.c in the Linux kernel before 4.17.4 could result in local attackers being able to crash the kernel or potentially elevate privileges because kmalloc_array is not used.
CVE-2018-13785	In libpng 1.6.34, a wrong calculation of row_factor in the png_check_chunk_length function (pngrutil.c) may trigger an integer overflow and resultant divide-by-zero while processing a crafted PNG file, leading to a denial of service.
CVE-2018-13988	Poppler through 0.62 contains an out of bounds read vulnerability due to an incorrect memory access that is not mapped in its memory space, as demonstrated by pdfunite. This can result in memory corruption and denial of service. This may be exploitable when a victim opens a specially crafted PDF file.
CVE-2018-14349	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap/command.c mishandles a NO response without a message.
CVE-2018-14350	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap/message.c has a stack-based buffer overflow for a FETCH response with a long INTERNALDATE field.
CVE-2018-14351	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap/command.c mishandles a long IMAP status mailbox literal count size.
CVE-2018-14352	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap_quote_string in imap/util.c does not leave room for quote characters, leading to a stack-based buffer overflow.

CVE-2018-14353	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap_quote_string in imap/util.c has an integer underflow.
CVE-2018-14354	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. They allow remote IMAP servers to execute arbitrary commands via backquote characters, related to the mailboxes command associated with a manual subscription or unsubscription.
CVE-2018-14355	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap/util.c mishandles ".." directory traversal in a mailbox name.
CVE-2018-14356	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. pop.c mishandles a zero-length UID.
CVE-2018-14357	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. They allow remote IMAP servers to execute arbitrary commands via backquote characters, related to the mailboxes command associated with an automatic subscription.
CVE-2018-14358	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap/message.c has a stack-based buffer overflow for a FETCH response with a long RFC822.SIZE field.
CVE-2018-14359	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. They have a buffer overflow via base64 data.
CVE-2018-14362	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. pop.c does not forbid characters that may have unsafe interaction with message-cache pathnames, as demonstrated by a '/' character.
CVE-2018-14404	A NULL pointer dereference vulnerability exists in the xpath.c:xmlXPathCompOpEval() function of libxml2 through 2.9.8 when parsing an invalid XPath expression in the XPATH_OP_AND or XPATH_OP_OR case. Applications processing untrusted XSL format inputs with the use of the libxml2 library may be vulnerable to a denial of service attack due to a crash of the application.
CVE-2018-14424	The daemon in GDM through 3.29.1 does not properly unexport display objects from its D-Bus interface when they are destroyed, which allows a local attacker to trigger a use-after-free via a specially crafted sequence of D-Bus method calls, resulting in a denial of service or potential code execution.
CVE-2018-14434	ImageMagick 7.0.8-4 has a memory leak for a colormap in WriteMPCImage in coders/mpc.c.

CVE-2018-14435	ImageMagick 7.0.8-4 has a memory leak in DecodeImage in coders/pcd.c.
CVE-2018-14436	ImageMagick 7.0.8-4 has a memory leak in ReadMIFFImage in coders/miff.c.
CVE-2018-14437	ImageMagick 7.0.8-4 has a memory leak in parse8BIM in coders/meta.c.
CVE-2018-14526	An issue was discovered in rsn_supp/wpa.c in wpa_supplicant 2.0 through 2.6. Under certain conditions, the integrity of EAPOL-Key messages is not checked, leading to a decryption oracle. An attacker within range of the Access Point and client can abuse the vulnerability to recover sensitive information.
CVE-2018-14551	The ReadMATImageV4 function in coders/mat.c in ImageMagick 7.0.8-7 uses an uninitialized variable, leading to memory corruption.
CVE-2018-14567	libxml2 2.9.8, if --with-lzma is used, allows remote attackers to cause a denial of service (infinite loop) via a crafted XML file that triggers LZMA_MEMLIMIT_ERROR, as demonstrated by xmllint, a different vulnerability than CVE-2015-8035 and CVE-2018-9251.
CVE-2018-14574	django.middleware.common.CommonMiddleware in Django 1.11.x before 1.11.15 and 2.0.x before 2.0.8 has an Open Redirect.
CVE-2018-14598	An issue was discovered in XListExtensions in ListExt.c in libX11 through 1.6.5. A malicious server can send a reply in which the first string overflows, causing a variable to be set to NULL that will be freed later on, leading to DoS (segmentation fault).
CVE-2018-14599	An issue was discovered in libX11 through 1.6.5. The function XListExtensions in ListExt.c is vulnerable to an off-by-one error caused by malicious server responses, leading to DoS or possibly unspecified other impact.
CVE-2018-14600	An issue was discovered in libX11 through 1.6.5. The function XListExtensions in ListExt.c interprets a variable as signed instead of unsigned, resulting in an out-of-bounds write (of up to 128 bytes), leading to DoS or remote code execution.
CVE-2018-14622	A null-pointer dereference vulnerability was found in libtirpc before version 0.3.3-rc3. The return value of makefd_xprt() was not checked in all instances, which could lead to a crash when the server exhausted the maximum number of available file descriptors. A remote attacker could cause an rpc-based application to crash by flooding it with new connections.
CVE-2018-14629	A denial of service vulnerability was discovered in Samba's LDAP server before versions 4.7.12, 4.8.7, and 4.9.3. A CNAME loop could lead to infinite

	recursion in the server. An unprivileged local attacker could create such an entry, leading to denial of service.
CVE-2018-14645	A flaw was discovered in the HPACK decoder of HAProxy, before 1.8.14, that is used for HTTP/2. An out-of-bounds read access in hpack_valid_idx() resulted in a remote crash and denial of service.
CVE-2018-14647	Python's elementtree C accelerator failed to initialise Expat's hash salt during initialization. This could make it easy to conduct denial of service attacks against Expat by constructing an XML document that would cause pathological hash collisions in Expat's internal data structures, consuming large amounts CPU and RAM. Python 3.8, 3.7, 3.6, 3.5, 3.4, 2.7 are believed to be vulnerable.
CVE-2018-14665	A flaw was found in xorg-x11-server before 1.20.3. An incorrect permission check for -modulepath and -logfile options when starting Xorg. X server allows unprivileged users with the ability to log in to the system via physical console to escalate their privileges and run arbitrary code under root privileges.
CVE-2018-14679	An issue was discovered in mspack/chmd.c in libmspack before 0.7alpha. There is an off-by-one error in the CHM PMGI/PMGL chunk number validity checks, which could lead to denial of service (uninitialized data dereference and application crash).
CVE-2018-14680	An issue was discovered in mspack/chmd.c in libmspack before 0.7alpha. It does not reject blank CHM filenames.
CVE-2018-14681	An issue was discovered in kwajd_read_headers in mspack/kwajd.c in libmspack before 0.7alpha. Bad KWAJ file header extensions could cause a one or two byte overwrite.
CVE-2018-14682	An issue was discovered in mspack/chmd.c in libmspack before 0.7alpha. There is an off-by-one error in the TOLOWER() macro for CHM decompression.
CVE-2018-14851	exif_process_IFD_in_MAKERNOTE in ext/exif/exif.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG file.
CVE-2018-14883	An issue was discovered in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. An Integer Overflow leads to a heap-based buffer over-read in exif_thumbnail_extract of exif.c.
CVE-2018-15120	libpango in Pango 1.40.8 through 1.42.3, as used in hexchat and other products, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted text with invalid Unicode sequences.

CVE-2018-15378	A vulnerability in ClamAV versions prior to 0.100.2 could allow an attacker to cause a denial of service (DoS) condition. The vulnerability is due to an error related to the MEW unpacker within the "unmew11()" function (libclamav/mew.c), which can be exploited to trigger an invalid read memory access via a specially crafted EXE file.
CVE-2018-15853	Endless recursion exists in xkbcomp/expr.c in xkbcommon and libxkbcommon before 0.8.1, which could be used by local attackers to crash xkbcommon users by supplying a crafted keymap file that triggers boolean negation.
CVE-2018-15854	Unchecked NULL pointer usage in xkbcommon before 0.8.1 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file, because geometry tokens were desupported incorrectly.
CVE-2018-15855	Unchecked NULL pointer usage in xkbcommon before 0.8.1 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file, because the XkbFile for an xkb_geometry section was mishandled.
CVE-2018-15856	An infinite loop when reaching EOL unexpectedly in compose/parser.c (aka the keymap parser) in xkbcommon before 0.8.1 could be used by local attackers to cause a denial of service during parsing of crafted keymap files.
CVE-2018-15857	An invalid free in ExprAppendMultiKeysymList in xkbcomp/ast-build.c in xkbcommon before 0.8.1 could be used by local attackers to crash xkbcommon keymap parsers or possibly have unspecified other impact by supplying a crafted keymap file.
CVE-2018-15858	Unchecked NULL pointer usage when handling invalid aliases in CopyKeyAliasesToKeymap in xkbcomp/keycodes.c in xkbcommon before 0.8.1 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file.
CVE-2018-15859	Unchecked NULL pointer usage when parsing invalid atoms in ExprResolveLhs in xkbcomp/expr.c in xkbcommon before 0.8.2 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file, because lookup failures are mishandled.
CVE-2018-15861	Unchecked NULL pointer usage in ExprResolveLhs in xkbcomp/expr.c in xkbcommon before 0.8.2 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file that triggers an xkb_intern_atom failure.

CVE-2018-15862	Unchecked NULL pointer usage in LookupModMask in xkbcomp/expr.c in xkbcommon before 0.8.2 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file with invalid virtual modifiers.
CVE-2018-15863	Unchecked NULL pointer usage in ResolveStateAndPredicate in xkbcomp/compat.c in xkbcommon before 0.8.2 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file with a no-op modmask expression.
CVE-2018-15864	Unchecked NULL pointer usage in resolve_keysym in xkbcomp/parser.y in xkbcommon before 0.8.2 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file, because a map access attempt can occur for a map that was never created.
CVE-2018-15908	In Artifex Ghostscript 9.23 before 2018-08-23, attackers are able to supply malicious PostScript files to bypass .tempfile restrictions and write files.
CVE-2018-15909	In Artifex Ghostscript 9.23 before 2018-08-24, a type confusion using the .shfill operator could be used by attackers able to supply crafted PostScript files to crash the interpreter or potentially execute code.
CVE-2018-15910	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files could use a type confusion in the LockDistillerParams parameter to crash the interpreter or execute code.
CVE-2018-15911	In Artifex Ghostscript 9.23 before 2018-08-24, attackers able to supply crafted PostScript could use uninitialized memory access in the aesdecode operator to crash the interpreter or potentially execute code.
CVE-2018-15967	Adobe Flash Player versions 30.0.0.154 and earlier have a privilege escalation vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-15978	Flash Player versions 31.0.0.122 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-15981	Flash Player versions 31.0.0.148 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2018-16065	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16066	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the

	candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16067	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16068	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16069	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16070	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16071	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16073	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16074	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16075	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16076	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16077	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when

	announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16078	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16079	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16080	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16081	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16082	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16083	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16084	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16085	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16151	In verify_emsa_pkcs1_signature() in gmp_rsa_public_key.c in the gmp plugin in strongSwan 4.x and 5.x before 5.7.0, the RSA implementation based on GMP does not reject excess data after the encoded algorithm OID during PKCS#1 v1.5 signature verification. Similar to the flaw in the same version of strongSwan regarding digestAlgorithm.parameters,

	a remote attacker can forge signatures when small public exponents are being used, which could lead to impersonation when only an RSA signature is used for IKEv2 authentication.
CVE-2018-16152	In verify_emsa_pkcs1_signature() in gmp_rsa_public_key.c in the gmp plugin in strongSwan 4.x and 5.x before 5.7.0, the RSA implementation based on GMP does not reject excess data in the digestAlgorithm.parameters field during PKCS#1 v1.5 signature verification. Consequently, a remote attacker can forge signatures when small public exponents are being used, which could lead to impersonation when only an RSA signature is used for IKEv2 authentication. This is a variant of CVE-2006-4790 and CVE-2014-1568.
CVE-2018-16323	ReadXBMImage in coders/xbm.c in ImageMagick before 7.0.8-9 leaves data uninitialized when processing an XBM file that has a negative pixel value. If the affected code is used as a library loaded into a process that includes sensitive information, that information sometimes can be leaked via the image data.
CVE-2018-16395	An issue was discovered in the OpenSSL library in Ruby before 2.3.8, 2.4.x before 2.4.5, 2.5.x before 2.5.2, and 2.6.x before 2.6.0-preview3. When two OpenSSL::X509::Name objects are compared using ==, depending on the ordering, non-equal objects may return true. When the first argument is one character longer than the second, or the second argument contains a character that is one less than a character in the same position of the first argument, the result of == will be true. This could be leveraged to create an illegitimate certificate that may be accepted as legitimate and then used in signing or encryption operations.
CVE-2018-16396	An issue was discovered in Ruby before 2.3.8, 2.4.x before 2.4.5, 2.5.x before 2.5.2, and 2.6.x before 2.6.0-preview3. It does not taint strings that result from unpacking tainted strings with some formats.
CVE-2018-16435	Little CMS (aka Little Color Management System) 2.9 has an integer overflow in the AllocateDataSet function in cmscgats.c, leading to a heap-based buffer overflow in the SetData function via a crafted file in the second argument to cmsIT8LoadFromFile.
CVE-2018-16509	An issue was discovered in Artifex Ghostscript before 9.24. Incorrect "restoration of privilege" checking during handling of /invalidaccess exceptions could be used by attackers able to supply crafted PostScript to execute code using the "pipe" instruction.
CVE-2018-16510	An issue was discovered in Artifex Ghostscript before 9.24. Incorrect exec stack handling in the "CS" and

	"SC" PDF primitives could be used by remote attackers able to supply crafted PDFs to crash the interpreter or possibly have unspecified other impact.
CVE-2018-16511	An issue was discovered in Artifex Ghostscript before 9.24. A type confusion in "ztype" could be used by remote attackers able to supply crafted PostScript to crash the interpreter or possibly have unspecified other impact.
CVE-2018-16513	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files could use a type confusion in the setcolor function to crash the interpreter or possibly have unspecified other impact.
CVE-2018-16539	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files could use incorrect access checking in temp file handling to disclose contents of files on the system otherwise not readable.
CVE-2018-16540	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files to the builtin PDF14 converter could use a use-after-free in copydevice handling to crash the interpreter or possibly have unspecified other impact.
CVE-2018-16541	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files could use incorrect free logic in pagedevice replacement to crash the interpreter.
CVE-2018-16542	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files could use insufficient interpreter stack-size checking during error handling to crash the interpreter.
CVE-2018-16543	In Artifex Ghostscript before 9.24, gssetresolution and gsgetresolution allow attackers to have an unspecified impact.
CVE-2018-16585	An issue was discovered in Artifex Ghostscript before 9.24. The .setdistillerkeys PostScript command is accepted even though it is not intended for use during document processing (e.g., after the startup phase). This leads to memory corruption, allowing remote attackers able to supply crafted PostScript to crash the interpreter or possibly have unspecified other impact.
CVE-2018-16640	ImageMagick 7.0.8-5 has a memory leak vulnerability in the function ReadOneJNGImage in coders/png.c.
CVE-2018-16642	The function InsertRow in coders/cut.c in ImageMagick 7.0.7-37 allows remote attackers to cause a denial of service via a crafted image file due to an out-of-bounds write.
CVE-2018-16643	The functions ReadDCMImage in coders/dcm.c, ReadPWPImage in coders/pwp.c, ReadCALSImage in coders/cals.c, and ReadPICTImage in coders/pict.c in ImageMagick 7.0.8-4 do not check the return value

	of the fputc function, which allows remote attackers to cause a denial of service via a crafted image file.
CVE-2018-16644	There is a missing check for length in the functions ReadDCMImage of coders/dcm.c and ReadPICTImage of coders/pict.c in ImageMagick 7.0.8-11, which allows remote attackers to cause a denial of service via a crafted image.
CVE-2018-16645	There is an excessive memory allocation issue in the functions ReadBMPImage of coders/bmp.c and ReadDIBImage of coders/dib.c in ImageMagick 7.0.8-11, which allows remote attackers to cause a denial of service via a crafted image file.
CVE-2018-16646	In Poppler 0.68.0, the Parser::getObj() function in Parser.cc may cause infinite recursion via a crafted file. A remote attacker can leverage this for a DoS attack.
CVE-2018-16749	In ImageMagick 7.0.7-29 and earlier, a missing NULL check in ReadOneJNGImage in coders/png.c allows an attacker to cause a denial of service (WriteBlob assertion failure and application exit) via a crafted file.
CVE-2018-16750	In ImageMagick 7.0.7-29 and earlier, a memory leak in the formatIPTCfromBuffer function in coders/meta.c was found.
CVE-2018-16802	An issue was discovered in Artifex Ghostscript before 9.25. Incorrect "restoration of privilege" checking when running out of stack during exception handling could be used by attackers able to supply crafted PostScript to execute code using the "pipe" instruction. This is due to an incomplete fix for CVE-2018-16509.
CVE-2018-16841	Samba from version 4.3.0 and before versions 4.7.12, 4.8.7 and 4.9.3 are vulnerable to a denial of service. When configured to accept smart-card authentication, Samba's KDC will call talloc_free() twice on the same memory if the principal in a validly signed certificate does not match the principal in the AS-REQ. This is only possible after authentication with a trusted certificate. talloc is robust against further corruption from a double-free with talloc_free() and directly calls abort(), terminating the KDC process.
CVE-2018-16843	nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.
CVE-2018-16844	nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.

CVE-2018-16845	nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.
CVE-2018-16847	An OOB heap buffer r/w access issue was found in the NVM Express Controller emulation in QEMU. It could occur in nvme_cmb_ops routines in nvme device. A guest user/process could use this flaw to crash the QEMU process resulting in DoS or potentially run arbitrary code with privileges of the QEMU process.
CVE-2018-16850	postgresql before versions 11.1, 10.6 is vulnerable to a to SQL injection in pg_upgrade and pg_dump via CREATE TRIGGER ... REFERENCING. Using a purpose-crafted trigger definition, an attacker can cause arbitrary SQL statements to run, with superuser privileges.
CVE-2018-16851	Samba from version 4.0.0 and before versions 4.7.12, 4.8.7, 4.9.3 is vulnerable to a denial of service. During the processing of an LDAP search before Samba's AD DC returns the LDAP entries to the client, the entries are cached in a single memory object with a maximum size of 256MB. When this size is reached, the Samba process providing the LDAP service will follow the NULL pointer, terminating the process. There is no further vulnerability associated with this issue, merely a denial of service.
CVE-2018-17183	Artifex Ghostscript before 9.25 allowed a user-writable error exception table, which could be used by remote attackers able to supply crafted PostScript to potentially overwrite or replace error handlers to inject code.
CVE-2018-17294	The matchCurrentInput function inside lou_translateString.c of Liblouis prior to 3.7 does not check the input string's length, allowing attackers to cause a denial of service (application crash via out-of-bounds read) by crafting an input file with certain translation dictionaries.
CVE-2018-17336	UDisks 2.8.0 has a format string vulnerability in udisks_log in udiskslogging.c, allowing attackers to obtain sensitive information (stack contents), cause a denial of service (memory corruption), or possibly have unspecified other impact via a malformed filesystem label, as demonstrated by %d or %n substrings.

CVE-2018-17407	An issue was discovered in t1_check_unusual_charstring functions in writet1.c files in TeX Live before 2018-09-21. A buffer overflow in the handling of Type 1 fonts allows arbitrary code execution when a malicious font is loaded by one of the vulnerable tools: pdflatex, pdftex, dvips, or luatex.
CVE-2018-17462	Incorrect refcounting in AppCache in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to perform a sandbox escape via a crafted HTML page.
CVE-2018-17463	Incorrect side effect annotation in V8 in Google Chrome prior to 70.0.3538.64 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-17464	Incorrect handling of history on iOS in Navigation in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-17465	Incorrect implementation of object trimming in V8 in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2018-17466	Incorrect texture handling in Angle in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-17467	Insufficiently quick clearing of stale rendered content in Navigation in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-17468	Incorrect handling of timer information during navigation in Blink in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to obtain cross origin URLs via a crafted HTML page.
CVE-2018-17469	Incorrect handling of PDF filter chains in PDFium in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2018-17470	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-17471	Incorrect dialog placement in WebContents in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to obscure the full screen warning via a crafted HTML page.
CVE-2018-17473	Incorrect handling of confusable characters in Omnibox in Google Chrome prior to 70.0.3538.67 allowed a

	remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-17474	Use after free in HTMLImportsController in Blink in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-17475	Incorrect handling of history on iOS in Navigation in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-17476	Incorrect dialog placement in Cast UI in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to obscure the full screen warning via a crafted HTML page.
CVE-2018-17477	Incorrect dialog placement in Extensions in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of extension popups via a crafted HTML page.
CVE-2018-17478	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-17479	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-17540	The gmp plugin in strongSwan before 5.7.1 has a Buffer Overflow via a crafted certificate.
CVE-2018-17958	Qemu has a Buffer Overflow in rtl8139_do_receive in hw/net/rtl8139.c because an incorrect integer data type is used.
CVE-2018-17961	Artifex Ghostscript 9.25 and earlier allows attackers to bypass a sandbox protection mechanism via vectors involving errorhandler setup. NOTE: this issue exists because of an incomplete fix for CVE-2018-17183.
CVE-2018-17962	Qemu has a Buffer Overflow in pcnet_receive in hw/net/pcnet.c because an incorrect integer data type is used.
CVE-2018-17963	qemu_deliver_packet_iov in net/net.c in Qemu accepts packet sizes greater than INT_MAX, which allows attackers to cause a denial of service or possibly have unspecified other impact.
CVE-2018-18065	_set_key in agent/helpers/table_container.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an authenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.

CVE-2018-18073	Artifex Ghostscript allows attackers to bypass a sandbox protection mechanism by leveraging exposure of system operators in the saved execution stack in an error object.
CVE-2018-18284	Artifex Ghostscript 9.25 and earlier allows attackers to bypass a sandbox protection mechanism via vectors involving the 1Policy operator.
CVE-2018-18751	An issue was discovered in GNU gettext 0.19.8. There is a double free in default_add_message in read-catalog.c, related to an invalid free in po_gram_parse in po-gram-gen.y, as demonstrated by lt-msgfmt.
CVE-2018-18849	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-18954	The pnv_lpc_do_eccb function in hw/ppc/pnv_lpc.c in Qemu before 3.1 allows out-of-bounds write or read access to PowerNV memory.
CVE-2018-19058	An issue was discovered in Poppler 0.71.0. There is a reachable abort in Object.h, will lead to denial of service because EmbFile::save2 in FileSpec.cc lacks a stream check before saving an embedded file.
CVE-2018-19059	An issue was discovered in Poppler 0.71.0. There is a out-of-bounds read in EmbFile::save2 in FileSpec.cc, will lead to denial of service, as demonstrated by utils/pdfdetach.cc not validating embedded files before save attempts.
CVE-2018-19060	An issue was discovered in Poppler 0.71.0. There is a NULL pointer dereference in goo/GooString.h, will lead to denial of service, as demonstrated by utils/pdfdetach.cc not validating a filename of an embedded file before constructing a save path.
CVE-2018-19364	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-19409	An issue was discovered in Artifex Ghostscript before 9.26. LockSafetyParams is not checked correctly if another device is used.
CVE-2018-19475	psi/zdevice2.c in Artifex Ghostscript before 9.26 allows remote attackers to bypass intended access restrictions because available stack space is not checked when the device remains the same.
CVE-2018-19476	psi/zicc.c in Artifex Ghostscript before 9.26 allows remote attackers to bypass intended access restrictions because of a setcolorspace type confusion.

CVE-2018-19477	psi/zfjbig2.c in Artifex Ghostscript before 9.26 allows remote attackers to bypass intended access restrictions because of a JBIG2Decode type confusion.
CVE-2018-2755	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows unauthenticated 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 and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of MySQL Server. 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-2018-2758	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2759	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2761	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.9 (Availability impacts).

	CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2762	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2766	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2767	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. 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 read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).
CVE-2018-2769	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Pluggable Auth). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2771	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Locking). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to

	exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2773	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2775	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2776	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Group Replication GCS). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via XCom 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-2018-2777	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2778	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2779	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2780	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2781	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2782	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows

	low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2784	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2786	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-2787	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-2810	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL

	Server. CVSS 3.0 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-2018-2812	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-2813	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).
CVE-2018-2816	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2817	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2818	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2819	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2825	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Libraries). The supported version that is affected is Java SE: 10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 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-2018-2826	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Libraries). The supported version that is affected is Java SE: 10. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the

	vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 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-2018-2839	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2846	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2952	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Concurrency). Supported versions that are affected are Java SE: 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171; JRockit: R28.3.18. 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 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 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/ AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2018-2972	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). The supported version that is affected is Java SE: 10.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 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-2018-3054	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3056	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/ AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).
CVE-2018-3058	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: MyISAM). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized 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-2018-3060	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H).
CVE-2018-3061	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-3062	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows low privileged 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. 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-2018-3063	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.60 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVE-2018-3064	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-3065	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3066	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized 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 3.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N).
CVE-2018-3070	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-3071	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Audit Log). Supported versions that are affected are 5.7.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-3077	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3081	Vulnerability in the MySQL Client component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client as well as unauthorized update, insert or delete access to some of MySQL Client accessible data. CVSS 3.0 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-3133	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3136	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are

	Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability 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 3.4 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:L/A:N).
CVE-2018-3139	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability 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-2018-3143	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently

	repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3144	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Audit). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3149	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. 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 applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 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-2018-3150	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Utility). The supported version that is affected is Java SE: 11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data. Note: This vulnerability applies to Java deployments 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 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2018-3155	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. 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-2018-3156	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3161	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3162	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0

	Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3169	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 7u191, 8u182 and 11; Java SE Embedded: 8u181. 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 (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g. code installed by an administrator). CVSS 3.0 Base Score 8.3 (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-2018-3171	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-3173	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3174	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs).

	Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes 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 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H).
CVE-2018-3180	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JSSE). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SSL/TLS 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 as well as 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 applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L).
CVE-2018-3183	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Scripting). Supported versions that are affected are Java SE: 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. 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 applies to Java deployments, typically in

	clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 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-2018-3185	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-3187	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-3200	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3247	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Merge). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with

	network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-3251	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3276	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3277	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3278	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: RBR). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or

	frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3282	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Storage Engines). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3283	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Logging). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3284	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3620	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access via a terminal page fault and a side-channel analysis.
CVE-2018-3639	Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka Speculative Store Bypass (SSB), Variant 4.

CVE-2018-3640	Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis, aka Rogue System Register Read (RSRE), Variant 3a.
CVE-2018-3646	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access with guest OS privilege via a terminal page fault and a side-channel analysis.
CVE-2018-3693	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a speculative buffer overflow and side-channel analysis.
CVE-2018-3822	X-Pack Security versions 6.2.0, 6.2.1, and 6.2.2 are vulnerable to a user impersonation attack via incorrect XML canonicalization and DOM traversal. An attacker might have been able to impersonate a legitimate user if the SAML Identity Provider allows for self registration with arbitrary identifiers and the attacker can register an account which an identifier that shares a suffix with a legitimate account. Both of those conditions must be true in order to exploit this flaw.
CVE-2018-4117	An issue was discovered in certain Apple products. iOS before 11.3 is affected. Safari before 11.1 is affected. iCloud before 7.4 on Windows is affected. iTunes before 12.7.4 on Windows is affected. watchOS before 4.3 is affected. The issue involves the fetch API in the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.
CVE-2018-4180	It was discovered that CUPS allows non-root users to pass environment variables to CUPS backends. Affected backends use attacker-controlled environment variables without proper sanitization. A local attacker, who is part of one of the groups specified in the SystemGroups directive, could use the cupsctl binary to set SetEnv and PassEnv directives and potentially controls the flow of the affected backend, resulting in some cases in arbitrary code execution with root privileges.
CVE-2018-4181	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2018-4190	An issue was discovered in certain Apple products. iOS before 11.4 is affected. Safari before 11.1.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive credential information that is transmitted during a CSS mask-image fetch.
CVE-2018-4199	An issue was discovered in certain Apple products. iOS before 11.4 is affected. Safari before 11.1.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a crafted web site.
CVE-2018-4200	An issue was discovered in certain Apple products. iOS before 11.3.1 is affected. Safari before 11.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site that triggers a WebCore::jsElementScrollHeightGetter use-after-free.
CVE-2018-4218	An issue was discovered in certain Apple products. iOS before 11.4 is affected. Safari before 11.1.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4 is affected. watchOS before 4.3.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site that triggers an @generatorState use-after-free.
CVE-2018-4222	An issue was discovered in certain Apple products. iOS before 11.4 is affected. Safari before 11.1.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4 is affected. watchOS before 4.3.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code via a crafted web site that leverages a getWasmBufferFromValue out-of-bounds read during WebAssembly compilation.
CVE-2018-4232	An issue was discovered in certain Apple products. iOS before 11.4 is affected. Safari before 11.1.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to overwrite cookies via a crafted web site.

CVE-2018-4233	An issue was discovered in certain Apple products. iOS before 11.4 is affected. Safari before 11.1.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4 is affected. watchOS before 4.3.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2018-4246	An issue was discovered in certain Apple products. iOS before 11.4 is affected. Safari before 11.1.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4 is affected. watchOS before 4.3.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code via a crafted web site that leverages type confusion.
CVE-2018-4871	An Out-of-bounds Read issue was discovered in Adobe Flash Player before 28.0.0.137. This vulnerability occurs because of computation that reads data that is past the end of the target buffer. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure.
CVE-2018-4877	A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to a dangling pointer in the Primetime SDK related to media player's quality of service functionality. A successful attack can lead to arbitrary code execution.
CVE-2018-4878	A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to a dangling pointer in the Primetime SDK related to media player handling of listener objects. A successful attack can lead to arbitrary code execution. This was exploited in the wild in January and February 2018.
CVE-2018-4919	Adobe Flash Player versions 28.0.0.161 and earlier have an exploitable use after free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-4920	Adobe Flash Player versions 28.0.0.161 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-4932	Adobe Flash Player versions 29.0.0.113 and earlier have an exploitable Use-After-Free vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.

CVE-2018-4933	Adobe Flash Player versions 29.0.0.113 and earlier have an exploitable out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-4934	Adobe Flash Player versions 29.0.0.113 and earlier have an exploitable out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-4935	Adobe Flash Player versions 29.0.0.113 and earlier have an exploitable out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-4936	Adobe Flash Player versions 29.0.0.113 and earlier have an exploitable Heap Overflow vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-4937	Adobe Flash Player versions 29.0.0.113 and earlier have an exploitable out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-4944	Adobe Flash Player versions 29.0.0.140 and earlier have an exploitable type confusion vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-4945	Adobe Flash Player versions 29.0.0.171 and earlier have a Type Confusion vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-5000	Adobe Flash Player versions 29.0.0.171 and earlier have an Integer Overflow vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-5001	Adobe Flash Player versions 29.0.0.171 and earlier have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-5002	Adobe Flash Player versions 29.0.0.171 and earlier have a Stack-based buffer overflow vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-5007	Adobe Flash Player 30.0.0.113 and earlier versions have a Type Confusion vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-5008	Adobe Flash Player 30.0.0.113 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-5089	Memory safety bugs were reported in Firefox 57 and Firefox ESR 52.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be

	exploited to run arbitrary code. This vulnerability affects Thunderbird < 52.6, Firefox ESR < 52.6, and Firefox < 58.
CVE-2018-5125	Memory safety bugs were reported in Firefox 58 and Firefox ESR 52.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 52.7, Firefox ESR < 52.7, and Firefox < 59.
CVE-2018-5150	Memory safety bugs were reported in Firefox 59, Firefox ESR 52.7, and Thunderbird 52.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 52.8, Thunderbird ESR < 52.8, Firefox < 60, and Firefox ESR < 52.8.
CVE-2018-5151	Memory safety bugs were reported in Firefox 59. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 60.
CVE-2018-5152	WebExtensions with the appropriate permissions can attach content scripts to Mozilla sites such as accounts.firefox.com and listen to network traffic to the site through the "webRequest" API. For example, this allows for the interception of username and an encrypted password during login to Firefox Accounts. This issue does not expose synchronization traffic directly and is limited to the process of user login to the website and the data displayed to the user once logged in. This vulnerability affects Firefox < 60.
CVE-2018-5153	If websocket data is sent with mixed text and binary in a single message, the binary data can be corrupted. This can result in an out-of-bounds read with the read memory sent to the originating server in response. This vulnerability affects Firefox < 60.
CVE-2018-5154	A use-after-free vulnerability can occur while enumerating attributes during SVG animations with clip paths. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.8, Thunderbird ESR < 52.8, Firefox < 60, and Firefox ESR < 52.8.
CVE-2018-5155	A use-after-free vulnerability can occur while adjusting layout during SVG animations with text paths. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.8, Thunderbird ESR < 52.8, Firefox < 60, and Firefox ESR < 52.8.
CVE-2018-5156	A vulnerability can occur when capturing a media stream when the media source type is changed as the

	capture is occurring. This can result in stream data being cast to the wrong type causing a potentially exploitable crash. This vulnerability affects Thunderbird < 60, Firefox ESR < 60.1, Firefox ESR < 52.9, and Firefox < 61.
CVE-2018-5157	Same-origin protections for the PDF viewer can be bypassed, allowing a malicious site to intercept messages meant for the viewer. This could allow the site to retrieve PDF files restricted to viewing by an authenticated user on a third-party website. This vulnerability affects Firefox ESR < 52.8 and Firefox < 60.
CVE-2018-5158	The PDF viewer does not sufficiently sanitize PostScript calculator functions, allowing malicious JavaScript to be injected through a crafted PDF file. This JavaScript can then be run with the permissions of the PDF viewer by its worker. This vulnerability affects Firefox ESR < 52.8 and Firefox < 60.
CVE-2018-5159	An integer overflow can occur in the Skia library due to 32-bit integer use in an array without integer overflow checks, resulting in possible out-of-bounds writes. This could lead to a potentially exploitable crash triggerable by web content. This vulnerability affects Thunderbird < 52.8, Thunderbird ESR < 52.8, Firefox < 60, and Firefox ESR < 52.8.
CVE-2018-5160	WebRTC can use a "WrappedI420Buffer" pixel buffer but the owning image object can be freed while it is still in use. This can result in the WebRTC encoder using uninitialized memory, leading to a potentially exploitable crash. This vulnerability affects Firefox < 60.
CVE-2018-5161	Crafted message headers can cause a Thunderbird process to hang on receiving the message. This vulnerability affects Thunderbird ESR < 52.8 and Thunderbird < 52.8.
CVE-2018-5162	Plaintext of decrypted emails can leak through the src attribute of remote images, or links. This vulnerability affects Thunderbird ESR < 52.8 and Thunderbird < 52.8.
CVE-2018-5163	If a malicious attacker has used another vulnerability to gain full control over a content process, they may be able to replace the alternate data resources stored in the JavaScript Start-up Bytecode Cache (JSBC) for other JavaScript code. If the parent process then runs this replaced code, the executed script would be run with the parent process' privileges, escaping the sandbox on content processes. This vulnerability affects Firefox < 60.
CVE-2018-5164	Content Security Policy (CSP) is not applied correctly to all parts of multipart content sent with the "multipart/x-mixed-replace" MIME type. This could allow for script

	to run where CSP should block it, allowing for cross-site scripting (XSS) and other attacks. This vulnerability affects Firefox < 60.
CVE-2018-5166	WebExtensions can use request redirection and a "filterReponseData" filter to bypass host permission settings to redirect network traffic and access content from a host for which they do not have explicit user permission. This vulnerability affects Firefox < 60.
CVE-2018-5167	The web console and JavaScript debugger do not sanitize all output that can be hyperlinked. Both will display "chrome:" links as active, clickable hyperlinks in their output. Web sites should not be able to directly link to internal chrome pages. Additionally, the JavaScript debugger will display "javascript:" links, which users could be tricked into clicking by malicious sites. This vulnerability affects Firefox < 60.
CVE-2018-5168	Sites can bypass security checks on permissions to install lightweight themes by manipulating the "baseURI" property of the theme element. This could allow a malicious site to install a theme without user interaction which could contain offensive or embarrassing images. This vulnerability affects Thunderbird < 52.8, Thunderbird ESR < 52.8, Firefox < 60, and Firefox ESR < 52.8.
CVE-2018-5169	If manipulated hyperlinked text with "chrome:" URL contained in it is dragged and dropped on the "home" icon, the home page can be reset to include a normally-unlinkable chrome page as one of the home page tabs. This vulnerability affects Firefox < 60.
CVE-2018-5170	It is possible to spoof the filename of an attachment and display an arbitrary attachment name. This could lead to a user opening a remote attachment which is a different file type than expected. This vulnerability affects Thunderbird ESR < 52.8 and Thunderbird < 52.8.
CVE-2018-5172	The Live Bookmarks page and the PDF viewer can run injected script content if a user pastes script from the clipboard into them while viewing RSS feeds or PDF files. This could allow a malicious site to socially engineer a user to copy and paste malicious script content that could then run with the context of either page but does not allow for privilege escalation. This vulnerability affects Firefox < 60.
CVE-2018-5173	The filename appearing in the "Downloads" panel improperly renders some Unicode characters, allowing for the file name to be spoofed. This can be used to obscure the file extension of potentially executable files from user view in the panel. Note: the dialog to open the file will show the full, correct filename and whether it is executable or not. This vulnerability affects Firefox < 60.

CVE-2018-5175	A mechanism to bypass Content Security Policy (CSP) protections on sites that have a "script-src" policy of "'strict-dynamic'". If a target website contains an HTML injection flaw an attacker could inject a reference to a copy of the "require.js" library that is part of Firefox's Developer Tools, and then use a known technique using that library to bypass the CSP restrictions on executing injected scripts. This vulnerability affects Firefox < 60.
CVE-2018-5176	The JSON Viewer displays clickable hyperlinks for strings that are parseable as URLs, including "javascript:" links. If a JSON file contains malicious JavaScript script embedded as "javascript:" links, users may be tricked into clicking and running this code in the context of the JSON Viewer. This can allow for the theft of cookies and authorization tokens which are accessible to that context. This vulnerability affects Firefox < 60.
CVE-2018-5177	A vulnerability exists in XSLT during number formatting where a negative buffer size may be allocated in some instances, leading to a buffer overflow and crash if it occurs. This vulnerability affects Firefox < 60.
CVE-2018-5178	A buffer overflow was found during UTF8 to Unicode string conversion within JavaScript with extremely large amounts of data. This vulnerability requires the use of a malicious or vulnerable legacy extension in order to occur. This vulnerability affects Thunderbird ESR < 52.8, Thunderbird < 52.8, and Firefox ESR < 52.8.
CVE-2018-5179	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-5180	A use-after-free vulnerability can occur during WebGL operations. While this results in a potentially exploitable crash, the vulnerability is limited because the memory is freed and reused in a brief window of time during the freeing of the same callstack. This vulnerability affects Firefox < 60.
CVE-2018-5181	If a URL using the "file:" protocol is dragged and dropped onto an open tab that is running in a different child process the tab will open a local file corresponding to the dropped URL, contrary to policy. One way to make the target tab open more reliably in a separate process is to open it with the "noopener" keyword. This vulnerability affects Firefox < 60.
CVE-2018-5182	If a text string that happens to be a filename in the operating system's native format is dragged and dropped onto the addressbar the specified local file will be opened. This is contrary to policy and is what would

	happen if the string were the equivalent "file:" URL. This vulnerability affects Firefox < 60.
CVE-2018-5183	Mozilla developers backported selected changes in the Skia library. These changes correct memory corruption issues including invalid buffer reads and writes during graphic operations. This vulnerability affects Thunderbird ESR < 52.8, Thunderbird < 52.8, and Firefox ESR < 52.8.
CVE-2018-5184	Using remote content in encrypted messages can lead to the disclosure of plaintext. This vulnerability affects Thunderbird ESR < 52.8 and Thunderbird < 52.8.
CVE-2018-5185	Plaintext of decrypted emails can leak through by user submitting an embedded form. This vulnerability affects Thunderbird ESR < 52.8 and Thunderbird < 52.8.
CVE-2018-5186	Memory safety bugs present in Firefox 60. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 61.
CVE-2018-5187	Memory safety bugs present in Firefox 60 and Firefox ESR 60. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 60, Firefox ESR < 60.1, and Firefox < 61.
CVE-2018-5188	Memory safety bugs present in Firefox 60, Firefox ESR 60, and Firefox ESR 52.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 60, Thunderbird < 52.9, Firefox ESR < 60.1, Firefox ESR < 52.9, and Firefox < 61.
CVE-2018-5246	In ImageMagick 7.0.7-17 Q16, there are memory leaks in ReadPATTERNImage in coders/pattern.c.
CVE-2018-5247	In ImageMagick 7.0.7-17 Q16, there are memory leaks in ReadRLAImage in coders/rla.c.
CVE-2018-5248	In ImageMagick 7.0.7-17 Q16, there is a heap-based buffer over-read in coders/sixel.c in the ReadSIXELImage function, related to the sixel_decode function.
CVE-2018-5357	ImageMagick 7.0.7-22 Q16 has memory leaks in the ReadDCMImage function in coders/dcm.c.
CVE-2018-5358	ImageMagick 7.0.7-22 Q16 has memory leaks in the EncodeImageAttributes function in coders/json.c, as demonstrated by the ReadPSDLayersInternal function in coders/psd.c.
CVE-2018-5388	In stroke_socket.c in strongSwan before 5.6.3, a missing packet length check could allow a buffer

	underflow, which may lead to resource exhaustion and denial of service while reading from the socket.
CVE-2018-5390	Linux kernel versions 4.9+ can be forced to make very expensive calls to tcp_collapse_ofo_queue() and tcp_prune_ofo_queue() for every incoming packet which can lead to a denial of service.
CVE-2018-5391	The Linux kernel, versions 3.9+, is vulnerable to a denial of service attack with low rates of specially modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service condition by sending specially crafted IP fragments. Various vulnerabilities in IP fragmentation have been discovered and fixed over the years. The current vulnerability (CVE-2018-5391) became exploitable in the Linux kernel with the increase of the IP fragment reassembly queue size.
CVE-2018-5711	gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1, has an integer signedness error that leads to an infinite loop via a crafted GIF file, as demonstrated by a call to the imagecreatefromgif or imagecreatefromstring PHP function. This is related to GetCode_ and gdImageCreateFromGifCtx.
CVE-2018-5738	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-5740	A denial of service flaw was discovered in bind versions that include the "deny-answer-aliases" feature. This flaw may allow a remote attacker to trigger an INSIST assert in named leading to termination of the process and a denial of service condition.
CVE-2018-5807	An error within the "samsung_load_raw()" function (internal/dcraw_common.cpp) in LibRaw versions prior to 0.18.9 can be exploited to cause an out-of-bounds read memory access and subsequently cause a crash.
CVE-2018-5810	An error within the "rollei_load_raw()" function (internal/dcraw_common.cpp) in LibRaw versions prior to 0.18.9 can be exploited to cause a heap-based buffer overflow and subsequently cause a crash.
CVE-2018-5811	An error within the "nikon_coolscan_load_raw()" function (internal/dcraw_common.cpp) in LibRaw versions prior to 0.18.9 can be exploited to cause an out-of-bounds read memory access and subsequently cause a crash.
CVE-2018-5812	An error within the "nikon_coolscan_load_raw()" function (internal/dcraw_common.cpp) in LibRaw

	versions prior to 0.18.9 can be exploited to trigger a NULL pointer dereference.
CVE-2018-5813	An error within the "parse_minolta()" function (dcraw/dcraw.c) in LibRaw versions prior to 0.18.11 can be exploited to trigger an infinite loop via a specially crafted file.
CVE-2018-5814	In the Linux Kernel before version 4.16.11, 4.14.43, 4.9.102, and 4.4.133, multiple race condition errors when handling probe, disconnect, and rebind operations can be exploited to trigger a use-after-free condition or a NULL pointer dereference by sending multiple USB over IP packets.
CVE-2018-5815	An integer overflow error within the "parse_qt()" function (internal/dcraw_common.cpp) in LibRaw versions prior to 0.18.12 can be exploited to trigger an infinite loop via a specially crafted Apple QuickTime file.
CVE-2018-5816	An integer overflow error within the "identify()" function (internal/dcraw_common.cpp) in LibRaw versions prior to 0.18.12 can be exploited to trigger a division by zero via specially crafted NOKIARAW file (Note: This vulnerability is caused due to an incomplete fix of CVE-2018-5804).
CVE-2018-6031	Use after free in PDFium in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2018-6032	Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user cross-origin data via a crafted HTML page.
CVE-2018-6033	Insufficient data validation in Downloads in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially run arbitrary code outside sandbox via a crafted Chrome Extension.
CVE-2018-6034	Insufficient data validation in WebGL in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6035	Insufficient policy enforcement in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user local file data via a crafted Chrome Extension.
CVE-2018-6036	Insufficient data validation in V8 in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user data via a crafted HTML page.
CVE-2018-6037	Inappropriate implementation in autofill in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to obtain autofill data with insufficient user gestures via a crafted HTML page.

CVE-2018-6038	Heap buffer overflow in WebGL in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6039	Insufficient data validation in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user cross-origin data via a crafted Chrome Extension.
CVE-2018-6040	Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially bypass content security policy via a crafted HTML page.
CVE-2018-6041	Incorrect security UI in navigation in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6042	Incorrect security UI in Omnibox in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6043	Insufficient data validation in External Protocol Handler in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially execute arbitrary programs on user machine via a crafted HTML page.
CVE-2018-6044	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6045	Insufficient policy enforcement in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user local file data via a crafted Chrome Extension.
CVE-2018-6046	Insufficient data validation in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user cross-origin data via a crafted Chrome Extension.
CVE-2018-6047	Insufficient policy enforcement in WebGL in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user redirect URL via a crafted HTML page.
CVE-2018-6048	Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak referrer information via a crafted HTML page.
CVE-2018-6049	Incorrect security UI in permissions prompt in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the origin to which permission is granted via a crafted HTML page.

CVE-2018-6050	Incorrect security UI in Omnibox in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6051	XSS Auditor in Google Chrome prior to 64.0.3282.119, did not ensure the reporting URL was in the same origin as the page it was on, which allowed a remote attacker to obtain referrer details via a crafted HTML page.
CVE-2018-6052	Lack of support for a non standard no-referrer policy value in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to obtain referrer details from a web page that had thought it had opted out of sending referrer data.
CVE-2018-6053	Inappropriate implementation in New Tab Page in Google Chrome prior to 64.0.3282.119 allowed a local attacker to view website thumbnail images after clearing browser data via a crafted HTML page.
CVE-2018-6054	Use after free in WebUI in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2018-6055	Insufficient policy enforcement in Catalog Service in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially run arbitrary code outside sandbox via a crafted HTML page.
CVE-2018-6056	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6057	Lack of special casing of Android ashmem in Google Chrome prior to 65.0.3325.146 allowed a remote attacker who had compromised the renderer process to bypass inter-process read only guarantees via a crafted HTML page.
CVE-2018-6058	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6059	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6060	Use after free in WebAudio in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6061	A race in the handling of SharedArrayBuffers in WebAssembly in Google Chrome prior to

	65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6062	Heap overflow write in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6063	Incorrect use of mojo::WrapSharedMemoryHandle in Mojo in Google Chrome prior to 65.0.3325.146 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6064	Type Confusion in the implementation of __defineGetter__ in V8 in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6065	Integer overflow in computing the required allocation size when instantiating a new javascript object in V8 in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6066	Lack of CORS checking by ResourceFetcher/ ResourceLoader in Blink in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6067	Incorrect IPC serialization in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6068	Object lifecycle issue in Chrome Custom Tab in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6069	Stack buffer overflow in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6070	Lack of CSP enforcement on WebUI pages in Bink in Google Chrome prior to 65.0.3325.146 allowed an attacker who convinced a user to install a malicious extension to bypass content security policy via a crafted Chrome Extension.
CVE-2018-6071	An integer overflow in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6072	An integer overflow leading to use after free in PDFium in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2018-6073	A heap buffer overflow in WebGL in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to

	perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6074	Failure to apply Mark-of-the-Web in Downloads in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to bypass OS level controls via a crafted HTML page.
CVE-2018-6075	Incorrect handling of specified filenames in file downloads in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page and user interaction.
CVE-2018-6076	Insufficient encoding of URL fragment identifiers in Blink in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform a DOM based XSS attack via a crafted HTML page.
CVE-2018-6077	Displacement map filters being applied to cross-origin images in Blink SVG rendering in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6078	Incorrect handling of confusable characters in Omnibox in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-6079	Inappropriate sharing of TEXTURE_2D_ARRAY/ TEXTURE_3D data between tabs in WebGL in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6080	Lack of access control checks in Instrumentation in Google Chrome prior to 65.0.3325.146 allowed a remote attacker who had compromised the renderer process to obtain memory metadata from privileged processes .
CVE-2018-6081	XSS vulnerabilities in Interstitials in Google Chrome prior to 65.0.3325.146 allowed an attacker who convinced a user to install a malicious extension or open Developer Console to inject arbitrary scripts or HTML via a crafted HTML page.
CVE-2018-6082	Including port 22 in the list of allowed FTP ports in Networking in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially enumerate internal host services via a crafted HTML page.
CVE-2018-6083	Failure to disallow PWA installation from CSP sandboxed pages in AppManifest in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to access privileged APIs via a crafted HTML page.
CVE-2018-6085	Re-entry of a destructor in Networking Disk Cache in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to execute arbitrary code via a crafted HTML page.

CVE-2018-6086	A double-eviction in the Incognito mode cache that lead to a user-after-free in Networking Disk Cache in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2018-6087	A use-after-free in WebAssembly in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-6088	An iterator-invalidation bug in PDFium in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.
CVE-2018-6089	A lack of CORS checks, after a Service Worker redirected to a cross-origin PDF, in Service Worker in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to leak limited cross-origin data via a crafted HTML page.
CVE-2018-6090	An integer overflow that lead to a heap buffer-overflow in Skia in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-6091	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6092	An integer overflow on 32-bit systems in WebAssembly in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-6093	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6094	Inline metadata in GarbageCollection in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6095	Inappropriate dismissal of file picker on keyboard events in Blink in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to read local files via a crafted HTML page.
CVE-2018-6096	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2018-6097	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6098	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6099	A lack of CORS checks in Blink in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to leak limited cross-origin data via a crafted HTML page.
CVE-2018-6100	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6101	A lack of host validation in DevTools in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to execute arbitrary code via a crafted HTML page, if the user is running a remote DevTools debugging server.
CVE-2018-6102	Missing confusable characters in Internationalization in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-6103	A stagnant permission prompt in Prompts in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to bypass permission policy via a crafted HTML page.
CVE-2018-6104	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6105	Incorrect handling of confusable characters in Omnibox in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6106	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6107	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6108	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.106

	allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted HTML page.
CVE-2018-6109	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6110	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6111	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6112	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6113	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6114	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6115	Inappropriate setting of the SEE_MASK_FLAG_NO_UI flag in file downloads in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to potentially bypass OS malware checks via a crafted HTML page.
CVE-2018-6116	A nullptr dereference in WebAssembly in Google Chrome prior to 66.0.3359.106 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2018-6117	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6119	Incorrect security UI in Omnibox in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.

CVE-2018-6120	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6121	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6122	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6123	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6124	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6125	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6126	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6127	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6128	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6129	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the

	candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6130	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6131	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6132	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6133	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6134	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6135	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6136	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6137	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6138	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6139	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when

	announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6140	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6141	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6142	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6143	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6144	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6145	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6147	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6148	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6149	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2018-6150	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6151	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6152	The implementation of the Page.downloadBehavior backend unconditionally marked downloaded files as safe, regardless of file type in Google Chrome prior to 66.0.3359.106 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted HTML page and user interaction.
CVE-2018-6153	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6154	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6155	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6156	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6157	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6158	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6159	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the

	candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6161	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6162	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6163	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6164	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6165	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6166	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6167	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6168	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6169	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6170	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when

	announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6171	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6172	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6173	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6174	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6175	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6176	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6177	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6178	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6179	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2018-6381	In ZZIPlib 0.13.67, there is a segmentation fault caused by invalid memory access in the zzip_disk_fread function (zzip/mmapped.c) because the size variable is not validated against the amount of file->stored data.
CVE-2018-6405	In the ReadDCMImage function in coders/dcm.c in ImageMagick before 7.0.7-23, each redmap, greenmap, and bluemap variable can be overwritten by a new pointer. The previous pointer is lost, which leads to a memory leak. This allows remote attackers to cause a denial of service.
CVE-2018-6484	In ZZIPlib 0.13.67, there is a memory alignment error and bus error in the __zzip_fetch_disk_trailer function of zzip/zip.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted zip file.
CVE-2018-6540	In ZZIPlib 0.13.67, there is a bus error caused by loading of a misaligned address in the zzip_disk_findfirst function of zzip/mmapped.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted zip file.
CVE-2018-6541	In ZZIPlib 0.13.67, there is a bus error caused by loading of a misaligned address (when handling disk64_trailer local entries) in __zzip_fetch_disk_trailer (zzip/zip.c). Remote attackers could leverage this vulnerability to cause a denial of service via a crafted zip file.
CVE-2018-6552	Apport does not properly handle crashes originating from a PID namespace allowing local users to create certain files as root which an attacker could leverage to perform a denial of service via resource exhaustion, possibly gain root privileges, or escape from containers. The is_same_ns() function returns True when /proc/<global pid>/ does not exist in order to indicate that the crash should be handled in the global namespace rather than inside of a container. However, the portion of the data/apport code that decides whether or not to forward a crash to a container does not always replace sys.argv[1] with the value stored in the host_pid variable when /proc/<global pid>/ does not exist which results in the container pid being used in the global namespace. This flaw affects versions 2.20.8-0ubuntu4 through 2.20.9-0ubuntu7, 2.20.7-0ubuntu3.7, 2.20.7-0ubuntu3.8, 2.20.1-0ubuntu2.15 through 2.20.1-0ubuntu2.17, and 2.14.1-0ubuntu3.28.
CVE-2018-6553	The CUPS AppArmor profile incorrectly confined the dnssd backend due to use of hard links. A local attacker could possibly use this issue to escape confinement. This flaw affects versions prior to 2.2.7-1ubuntu2.1 in Ubuntu 18.04 LTS, prior to 2.2.4-7ubuntu3.1 in Ubuntu 17.10, prior to 2.1.3-4ubuntu0.5 in Ubuntu 16.04 LTS, and prior to 1.7.2-0ubuntu1.10 in Ubuntu 14.04 LTS.

CVE-2018-6556	lxc-user-nic when asked to delete a network interface will unconditionally open a user provided path. This code path may be used by an unprivileged user to check for the existence of a path which they wouldn't otherwise be able to reach. It may also be used to trigger side effects by causing a (read-only) open of special kernel files (ptmx, proc, sys). Affected releases are LXC: 2.0 versions above and including 2.0.9; 3.0 versions above and including 3.0.0, prior to 3.0.2.
CVE-2018-6557	The MOTD update script in the base-files package in Ubuntu 18.04 LTS before 10.1ubuntu2.2, and Ubuntu 18.10 before 10.1ubuntu6 incorrectly handled temporary files. A local attacker could use this issue to cause a denial of service, or possibly escalate privileges if kernel symlink restrictions were disabled.
CVE-2018-6869	In ZZIPlib 0.13.68, there is an uncontrolled memory allocation and a crash in the __zzip_parse_root_directory function of zzip/zip.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted zip file.
CVE-2018-7182	The ctl_getitem method in ntpd in ntp-4.2.8p6 before 4.2.8p11 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mode 6 packet with a ntpd instance from 4.2.8p6 through 4.2.8p10.
CVE-2018-7183	Buffer overflow in the decodearr function in ntpq in ntp 4.2.8p6 through 4.2.8p10 allows remote attackers to execute arbitrary code by leveraging an ntpq query and sending a response with a crafted array.
CVE-2018-7184	ntpd in ntp 4.2.8p4 before 4.2.8p11 drops bad packets before updating the "received" timestamp, which allows remote attackers to cause a denial of service (disruption) by sending a packet with a zero-origin timestamp causing the association to reset and setting the contents of the packet as the most recent timestamp. This issue is a result of an incomplete fix for CVE-2015-7704.
CVE-2018-7185	The protocol engine in ntp 4.2.6 before 4.2.8p11 allows a remote attackers to cause a denial of service (disruption) by continually sending a packet with a zero-origin timestamp and source IP address of the "other side" of an interleaved association causing the victim ntpd to reset its association.
CVE-2018-7443	The ReadTIFFImage function in coders/tiff.c in ImageMagick 7.0.7-23 Q16 does not properly validate the amount of image data in a file, which allows remote attackers to cause a denial of service (memory allocation failure in the AcquireMagickMemory function in MagickCore/memory.c).

CVE-2018-7550	The load_multiboot function in hw/i386/multiboot.c in Quick Emulator (aka QEMU) allows local guest OS users to execute arbitrary code on the QEMU host via a mh_load_end_addr value greater than mh_bss_end_addr, which triggers an out-of-bounds read or write memory access.
CVE-2018-7725	An issue was discovered in ZZIPlib 0.13.68. An invalid memory address dereference was discovered in zzip_disk_fread in mmapped.c. The vulnerability causes an application crash, which leads to denial of service.
CVE-2018-7726	An issue was discovered in ZZIPlib 0.13.68. There is a bus error caused by the __zzip_parse_root_directory function of zip.c. Attackers could leverage this vulnerability to cause a denial of service via a crafted zip file.
CVE-2018-7755	An issue was discovered in the fd_locked_ioctl function in drivers/block/floppy.c in the Linux kernel through 4.15.7. The floppy driver will copy a kernel pointer to user memory in response to the FDGETPRM ioctl. An attacker can send the FDGETPRM ioctl and use the obtained kernel pointer to discover the location of kernel code and data and bypass kernel security protections such as KASLR.
CVE-2018-7858	Quick Emulator (aka QEMU), when built with the Cirrus CLGD 54xx VGA Emulator support, allows local guest OS privileged users to cause a denial of service (out-of-bounds access and QEMU process crash) by leveraging incorrect region calculation when updating VGA display.
CVE-2018-8014	The defaults settings for the CORS filter provided in Apache Tomcat 9.0.0.M1 to 9.0.8, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52, 7.0.41 to 7.0.88 are insecure and enable 'supportsCredentials' for all origins. It is expected that users of the CORS filter will have configured it appropriately for their environment rather than using it in the default configuration. Therefore, it is expected that most users will not be impacted by this issue.
CVE-2018-8087	Memory leak in the hwsim_new_radio_nl function in drivers/net/wireless/mac80211_hwsim.c in the Linux kernel through 4.15.9 allows local users to cause a denial of service (memory consumption) by triggering an out-of-array error case.
CVE-2018-8804	WriteEPTImage in coders/ept.c in ImageMagick 7.0.7-25 Q16 allows remote attackers to cause a denial of service (MagickCore/memory.c double free and application crash) or possibly have unspecified other impact via a crafted file.
CVE-2018-8960	The ReadTIFFImage function in coders/tiff.c in ImageMagick 7.0.7-26 Q16 does not properly restrict

	memory allocation, leading to a heap-based buffer over-read.
CVE-2018-9133	ImageMagick 7.0.7-26 Q16 has excessive iteration in the DecodeLabImage and EncodeLabImage functions (coders/tiff.c), which results in a hang (tens of minutes) with a tiny PoC file. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted tiff file.
CVE-2018-9234	GnuPG 2.2.4 and 2.2.5 does not enforce a configuration in which key certification requires an offline master Certify key, which results in apparently valid certifications that occurred only with access to a signing subkey.
CVE-2018-9415	In driver_override_store and driver_override_show of bus.c, there is a possible double free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-69129004 References: Upstream kernel.

5.2 Passed rules - Security Best Practices-1.0

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

Support SSH Version 2 Only	This rule helps determine whether your EC2 instances are configured to support SSH protocol version 1.0.