



Amazon Inspector - Assessment Report

Full Report

Report generated on 2022-09-05 at 07:51:52 UTC

Assessment Template: AWS-INSPECTOR-AMI-TESTING-ASSESSMENT

Assessment Run start: 2022-09-05 at 07:04:23 UTC
Assessment Run end: 2022-09-05 at 07:21:03 UTC

Section 1: Executive Summary

This is an Inspector assessment report for an assessment started on 2022-09-05 07:04:23 UTC for assessment template 'AWS-INSPECTOR-AMI-TESTING-ASSESSMENT'. The assessment target included 1 instances, and was tested against 4 Rules Packages.

The assessment target is defined using the following EC2 tags

Key	Value
env	production

The following Rules Packages were assessed. A total of 183 findings were created, with the following distribution by severity:

Rules Package	High	Medium	Low	Informational
CIS Operating System Security Configuration Benchmarks-1.0	88	0	0	8
Common Vulnerabilities and Exposures-1.1	3	4	1	0
Network Reachability-1.1	0	0	2	76
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: 4

2.1.1: CIS Operating System Security Configuration Benchmarks-1.0

Description: The CIS Security Benchmarks program provides well-defined, unbiased and consensus-based industry best practices to help organizations assess and improve their security.

The rules in this package help establish a secure configuration posture for the following operating systems:

- Amazon Linux 2 (CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 1)
- Amazon Linux 2 (CIS Benchmark for Amazon Linux 2 Benchmark v1.0.0 Level 2)
- Ubuntu Linux 18.04 LTS (CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Server)
- Ubuntu Linux 18.04 LTS (CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Server)
- Ubuntu Linux 18.04 LTS (CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 1 Workstation)
- Ubuntu Linux 18.04 LTS (CIS Benchmark for Ubuntu Linux 18.04 LTS Benchmark v1.0.0 Level 2 Workstation)
- Amazon Linux version 2015.03 (CIS benchmark v1.1.0)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Domain Controller)
- Windows Server 2008 R2 (CIS Benchmark for Microsoft Windows 2008 R2, v3.0.0, Level 1 Member Server Profile)

- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows Server 2012 R2, v2.2.0, Level 1 Member Server Profile)
- Windows Server 2012 R2 (CIS Benchmark for Microsoft Windows Server 2012 R2, v2.2.0, Level 1 Domain Controller Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows Server 2012 non-R2, v2.0.0, Level 1 Member Server Profile)
- Windows Server 2012 (CIS Benchmark for Microsoft Windows Server 2012 non-R2, v2.0.0, Level 1 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows Server 2016 RTM (Release 1607), v1.1.0, Level 1 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows Server 2016 RTM (Release 1607), v1.1.0, Level 2 Member Server Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows Server 2016 RTM (Release 1607), v1.1.0, Level 1 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows Server 2016 RTM (Release 1607), v1.1.0, Level 2 Domain Controller Profile)
- Windows Server 2016 (CIS Benchmark for Microsoft Windows Server 2016 RTM (Release 1607), v1.1.0, Next Generation Windows Security Profile)
- Amazon Linux (CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 1)
- Amazon Linux (CIS Benchmark for Amazon Linux Benchmark v2.1.0 Level 2)
- CentOS Linux 7 (CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Server)
- CentOS Linux 7 (CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Server)
- CentOS Linux 7 (CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 1 Workstation)
- CentOS Linux 7 (CIS Benchmark for CentOS Linux 7 Benchmark v2.2.0 Level 2 Workstation)
- Red Hat Enterprise Linux 7 (CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Server)
- Red Hat Enterprise Linux 7 (CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Server)
- Red Hat Enterprise Linux 7 (CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 1 Workstation)
- Red Hat Enterprise Linux 7 (CIS Benchmark for Red Hat Enterprise Linux 7 Benchmark v2.1.1 Level 2 Workstation)

- Ubuntu Linux 16.04 LTS (CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Server)
- Ubuntu Linux 16.04 LTS (CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Server)
- Ubuntu Linux 16.04 LTS (CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 1 Workstation)
- Ubuntu Linux 16.04 LTS (CIS Benchmark for Ubuntu Linux 16.04 LTS Benchmark v1.1.0 Level 2 Workstation)
- CentOS Linux 6 (CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2, Level 1 Server)
- CentOS Linux 6 (CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2, Level 2 Server)
- CentOS Linux 6 (CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2, Level 1 Workstation)
- CentOS Linux 6 (CIS Benchmark for CentOS Linux 6 Benchmark v2.0.2, Level 2 Workstation)
- Red Hat Enterprise Linux 6 (CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2, Level 1 Server)
- Red Hat Enterprise Linux 6 (CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2, Level 2 Server)
- Red Hat Enterprise Linux 6 (CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2, Level 1 Workstation)
- Red Hat Enterprise Linux 6 (CIS Benchmark for Red Hat Enterprise Linux 6 Benchmark v2.0.2 Level 2 Workstation)
- Ubuntu Linux 14.04 LTS (CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0, Level 1 Server)
- Ubuntu Linux 14.04 LTS (CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0, Level 2 Server)
- Ubuntu Linux 14.04 LTS (CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0, Level 1 Workstation)
- Ubuntu Linux 14.04 LTS (CIS Benchmark for Ubuntu Linux 14.04 LTS Benchmark v2.0.0, Level 2 Workstation)

If a particular CIS benchmark appears in a finding produced by an Amazon Inspector assessment run, you can download a detailed PDF description of the benchmark from <https://benchmarks.cisecurity.org/> (free registration

required). The benchmark document provides detailed information about this CIS benchmark, its severity, and how to mitigate it.

Provider: Amazon Web Services, Inc.

Version: 1.0

2.1.2: 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

2.1.3: Network Reachability-1.1

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

Provider: Amazon Web Services, Inc.

Version: 1.1

2.1.4: 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 - AWS-INSPECTOR-AMI-TESTING-ASSESSMENT

2.2.1: EC2 Tags:

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

Key	Value
env	production

2.2.2: Instances - Count 1

Instance ID
i-079d0668bb45659b2

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 - CIS Operating System Security Configuration Benchmarks-1.0

3.1.1 Level 1

Rule	Severity	Failed
1.1.2 Ensure /tmp is configured	High	1
1.1.17 Ensure noexec option set on /dev/shm partition	High	1
1.1.1.1 Ensure mounting of cramfs filesystems is disabled	High	1
1.1.1.2 Ensure mounting of hfs filesystems is disabled	High	1
1.1.1.3 Ensure mounting of hfsplus filesystems is disabled	High	1
1.1.1.4 Ensure mounting of squashfs filesystems is disabled	High	1
1.1.1.5 Ensure mounting of udf filesystems is disabled	High	1
1.3.1 Ensure AIDE is installed	High	1
1.3.2 Ensure filesystem integrity is regularly checked	High	1
1.5.1 Ensure core dumps are restricted	High	1
1.5.2 Ensure address space layout randomization (ASLR) is enabled	High	1
1.7.1.1 Ensure message of the day is configured properly	High	1
1.7.1.2 Ensure local login warning banner is configured properly	Informational	1
1.7.1.3 Ensure remote login warning banner is configured properly	Informational	1
3.1.1 Ensure IP forwarding is disabled	High	1
3.1.2 Ensure packet redirect sending is disabled	High	1
3.2.1 Ensure source routed packets are not accepted	High	1
3.2.2 Ensure ICMP redirects are not accepted	High	1
3.2.3 Ensure secure ICMP redirects are not accepted	High	1
3.2.4 Ensure suspicious packets are logged	High	1
3.2.5 Ensure broadcast ICMP requests are ignored	High	1
3.2.6 Ensure bogus ICMP responses are ignored	High	1

3.2.7 Ensure Reverse Path Filtering is enabled	High	1
3.2.8 Ensure TCP SYN Cookies is enabled	High	1
3.2.9 Ensure IPv6 router advertisements are not accepted	High	1
3.3.3 Ensure /etc/hosts.deny is configured	Informational	1
3.4.1 Ensure DCCP is disabled	Informational	1
3.4.2 Ensure SCTP is disabled	Informational	1
3.4.3 Ensure RDS is disabled	Informational	1
3.4.4 Ensure TIPC is disabled	Informational	1
3.5.1.1 Ensure default deny firewall policy	High	1
3.5.1.2 Ensure loopback traffic is configured	High	1
3.5.1.4 Ensure firewall rules exist for all open ports	High	1
3.5.2.1 Ensure IPv6 default deny firewall policy	High	1
3.5.2.2 Ensure IPv6 loopback traffic is configured	High	1
4.2.4 Ensure permissions on all logfiles are configured	High	1
4.2.1.3 Ensure rsyslog default file permissions configured	High	1
4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host	High	1
5.6 Ensure access to the su command is restricted	High	1
5.1.2 Ensure permissions on /etc/crontab are configured	High	1
5.1.3 Ensure permissions on /etc/cron.hourly are configured	High	1
5.1.4 Ensure permissions on /etc/cron.daily are configured	High	1
5.1.5 Ensure permissions on /etc/cron.weekly are configured	High	1
5.1.6 Ensure permissions on /etc/cron.monthly are configured	High	1
5.1.7 Ensure permissions on /etc/cron.d are configured	High	1
5.1.8 Ensure at/cron is restricted to authorized users	High	1
5.2.4 Ensure SSH Protocol is set to 2	High	1
5.2.5 Ensure SSH LogLevel is appropriate	High	1
5.2.7 Ensure SSH MaxAuthTries is set to 4 or less	High	1
5.2.8 Ensure SSH IgnoreRhosts is enabled	High	1
5.2.9 Ensure SSH HostbasedAuthentication is disabled	High	1
5.2.10 Ensure SSH root login is disabled	High	1
5.2.11 Ensure SSH PermitEmptyPasswords is disabled	High	1
5.2.12 Ensure SSH PermitUserEnvironment is disabled	High	1
5.2.13 Ensure only strong ciphers are used	High	1
5.2.14 Ensure only strong MAC algorithms are used	High	1
5.2.15 Ensure that strong Key Exchange algorithms are used	High	1
5.2.16 Ensure SSH Idle Timeout Interval is configured	High	1
5.2.17 Ensure SSH LoginGraceTime is set to one minute or less	High	1
5.2.18 Ensure SSH access is limited	High	1
5.2.19 Ensure SSH warning banner is configured	High	1

5.3.1 Ensure password creation requirements are configured	High	1
5.3.2 Ensure lockout for failed password attempts is configured	High	1
5.3.3 Ensure password reuse is limited	High	1
5.4.4 Ensure default user umask is 027 or more restrictive	High	1
5.4.1.1 Ensure password expiration is 365 days or less	High	1
5.4.1.2 Ensure minimum days between password changes is 7 or more	High	1
5.4.1.4 Ensure inactive password lock is 30 days or less	High	1

3.1.2 Level 2

Rule	Severity	Failed
1.1.2 Ensure /tmp is configured	High	1
1.1.6 Ensure separate partition exists for /var	High	1
1.1.7 Ensure separate partition exists for /var/tmp	High	1
1.1.11 Ensure separate partition exists for /var/log	High	1
1.1.12 Ensure separate partition exists for /var/log/audit	High	1
1.1.13 Ensure separate partition exists for /home	High	1
1.1.17 Ensure noexec option set on /dev/shm partition	High	1
1.1.1.1 Ensure mounting of cramfs filesystems is disabled	High	1
1.1.1.2 Ensure mounting of hfs filesystems is disabled	High	1
1.1.1.3 Ensure mounting of hfsplus filesystems is disabled	High	1
1.1.1.4 Ensure mounting of squashfs filesystems is disabled	High	1
1.1.1.5 Ensure mounting of udf filesystems is disabled	High	1
1.3.1 Ensure AIDE is installed	High	1
1.3.2 Ensure filesystem integrity is regularly checked	High	1
1.5.1 Ensure core dumps are restricted	High	1
1.5.2 Ensure address space layout randomization (ASLR) is enabled	High	1
1.6.1.2 Ensure the SELinux state is enforcing	High	1
1.6.1.3 Ensure SELinux policy is configured	High	1
1.6.1.6 Ensure no unconfined daemons exist	High	1
1.7.1.1 Ensure message of the day is configured properly	High	1
1.7.1.2 Ensure local login warning banner is configured properly	Informational	1
1.7.1.3 Ensure remote login warning banner is configured properly	Informational	1
3.6 Disable IPv6	Informational	1
3.1.1 Ensure IP forwarding is disabled	High	1
3.1.2 Ensure packet redirect sending is disabled	High	1
3.2.1 Ensure source routed packets are not accepted	High	1
3.2.2 Ensure ICMP redirects are not accepted	High	1
3.2.3 Ensure secure ICMP redirects are not accepted	High	1

3.2.4 Ensure suspicious packets are logged	High	1
3.2.5 Ensure broadcast ICMP requests are ignored	High	1
3.2.6 Ensure bogus ICMP responses are ignored	High	1
3.2.7 Ensure Reverse Path Filtering is enabled	High	1
3.2.8 Ensure TCP SYN Cookies is enabled	High	1
3.2.9 Ensure IPv6 router advertisements are not accepted	High	1
3.3.3 Ensure /etc/hosts.deny is configured	Informational	1
3.4.1 Ensure DCCP is disabled	Informational	1
3.4.2 Ensure SCTP is disabled	Informational	1
3.4.3 Ensure RDS is disabled	Informational	1
3.4.4 Ensure TIPC is disabled	Informational	1
3.5.1.1 Ensure default deny firewall policy	High	1
3.5.1.2 Ensure loopback traffic is configured	High	1
3.5.1.4 Ensure firewall rules exist for all open ports	High	1
3.5.2.1 Ensure IPv6 default deny firewall policy	High	1
3.5.2.2 Ensure IPv6 loopback traffic is configured	High	1
4.1.3 Ensure auditing for processes that start prior to auditd is enabled	High	1
4.1.4 Ensure events that modify date and time information are collected	High	1
4.1.5 Ensure events that modify user/group information are collected	High	1
4.1.6 Ensure events that modify the system's network environment are collected	High	1
4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected	High	1
4.1.8 Ensure login and logout events are collected	High	1
4.1.9 Ensure session initiation information is collected	High	1
4.1.10 Ensure discretionary access control permission modification events are collected	High	1
4.1.11 Ensure unsuccessful unauthorized file access attempts are collected	High	1
4.1.13 Ensure successful file system mounts are collected	High	1
4.1.14 Ensure file deletion events by users are collected	High	1
4.1.15 Ensure changes to system administration scope (sudoers) is collected	High	1
4.1.16 Ensure system administrator actions (sudolog) are collected	High	1
4.1.17 Ensure kernel module loading and unloading is collected	High	1
4.1.18 Ensure the audit configuration is immutable	High	1
4.1.1.2 Ensure system is disabled when audit logs are full	High	1
4.1.1.3 Ensure audit logs are not automatically deleted	High	1
4.2.4 Ensure permissions on all logfiles are configured	High	1
4.2.1.3 Ensure rsyslog default file permissions configured	High	1

4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host	High	1
5.6 Ensure access to the su command is restricted	High	1
5.1.2 Ensure permissions on /etc/crontab are configured	High	1
5.1.3 Ensure permissions on /etc/cron.hourly are configured	High	1
5.1.4 Ensure permissions on /etc/cron.daily are configured	High	1
5.1.5 Ensure permissions on /etc/cron.weekly are configured	High	1
5.1.6 Ensure permissions on /etc/cron.monthly are configured	High	1
5.1.7 Ensure permissions on /etc/cron.d are configured	High	1
5.1.8 Ensure at/cron is restricted to authorized users	High	1
5.2.4 Ensure SSH Protocol is set to 2	High	1
5.2.5 Ensure SSH LogLevel is appropriate	High	1
5.2.6 Ensure SSH X11 forwarding is disabled	High	1
5.2.7 Ensure SSH MaxAuthTries is set to 4 or less	High	1
5.2.8 Ensure SSH IgnoreRhosts is enabled	High	1
5.2.9 Ensure SSH HostbasedAuthentication is disabled	High	1
5.2.10 Ensure SSH root login is disabled	High	1
5.2.11 Ensure SSH PermitEmptyPasswords is disabled	High	1
5.2.12 Ensure SSH PermitUserEnvironment is disabled	High	1
5.2.13 Ensure only strong ciphers are used	High	1
5.2.14 Ensure only strong MAC algorithms are used	High	1
5.2.15 Ensure that strong Key Exchange algorithms are used	High	1
5.2.16 Ensure SSH Idle Timeout Interval is configured	High	1
5.2.17 Ensure SSH LoginGraceTime is set to one minute or less	High	1
5.2.18 Ensure SSH access is limited	High	1
5.2.19 Ensure SSH warning banner is configured	High	1
5.3.1 Ensure password creation requirements are configured	High	1
5.3.2 Ensure lockout for failed password attempts is configured	High	1
5.3.3 Ensure password reuse is limited	High	1
5.4.4 Ensure default user umask is 027 or more restrictive	High	1
5.4.5 Ensure default user shell timeout is 900 seconds or less	High	1
5.4.1.1 Ensure password expiration is 365 days or less	High	1
5.4.1.2 Ensure minimum days between password changes is 7 or more	High	1
5.4.1.4 Ensure inactive password lock is 30 days or less	High	1

3.2: Findings table - Common Vulnerabilities and Exposures-1.1

Rule	Severity	Failed

CVE-2022-23825	Medium	1
CVE-2022-26373	Medium	1
CVE-2022-29900	Medium	1
CVE-2022-29901	Low	1
CVE-2022-34903	High	1
CVE-2022-36123	High	1
CVE-2022-36879	Medium	1
CVE-2022-36946	High	1

3.3: Findings table - Network Reachability-1.1

Rule	Severity	Failed
TCP port 111 (NFS) is reachable from the internet with active listener on instance	Informational	1
TCP port 111 (RPC) is reachable from the internet with active listener on instance	Informational	1
TCP port 1110 (NFS) is reachable from the internet with no listener on instance	Informational	1
TCP port 135 (RPC) is reachable from the internet with no listener on instance	Informational	1
TCP port 137 (NetBIOS) is reachable from the internet with no listener on instance	Informational	1
TCP port 139 (NetBIOS) is reachable from the internet with no listener on instance	Informational	1
TCP port 1433 (SQLServer) is reachable from the internet with no listener on instance	Informational	1
TCP port 1512 (WINS) is reachable from the internet with no listener on instance	Informational	1
TCP port 1521 (Oracle) is reachable from the internet with no listener on instance	Informational	1
TCP port 1630 (Oracle) is reachable from the internet with no listener on instance	Informational	1
TCP port 20 (FTP) is reachable from the internet with no listener on instance	Informational	1
TCP port 2049 (NFS) is reachable from the internet with no listener on instance	Informational	1
TCP port 21 (FTP) is reachable from the internet with no listener on instance	Informational	1
TCP port 22 (SSH) is reachable from the internet with active listener on instance	Informational	1
TCP port 23 (Telnet) is reachable from the internet with no listener on instance	Informational	1

TCP port 27017 (MongoDB) is reachable from the internet with no listener on instance	Informational	1
TCP port 27018 (MongoDB) is reachable from the internet with no listener on instance	Informational	1
TCP port 27019 (MongoDB) is reachable from the internet with no listener on instance	Informational	1
TCP port 28017 (MongoDB) is reachable from the internet with no listener on instance	Informational	1
TCP port 3268 (Global Catalog LDAP) is reachable from the internet with no listener on instance	Informational	1
TCP port 3269 (Global Catalog LDAP over TLS) is reachable from the internet with no listener on instance	Informational	1
TCP port 3306 (MySQL) is reachable from the internet with no listener on instance	Informational	1
TCP port 3389 (RDP) is reachable from the internet with no listener on instance	Informational	1
TCP port 389 (LDAP) is reachable from the internet with no listener on instance	Informational	1
TCP port 4045 (NFS) is reachable from the internet with no listener on instance	Informational	1
TCP port 42 (WINS) is reachable from the internet with no listener on instance	Informational	1
TCP port 443 (HTTPS) is reachable from the internet with no listener on instance	Informational	1
TCP port 445 (SMB) is reachable from the internet with no listener on instance	Informational	1
TCP port 464 (Kerberos) is reachable from the internet with no listener on instance	Informational	1
TCP port 515 (Print Services) is reachable from the internet with no listener on instance	Informational	1
TCP port 530 (RPC) is reachable from the internet with no listener on instance	Informational	1
TCP port 543 (Kerberos) is reachable from the internet with no listener on instance	Informational	1
TCP port 5432 (PostgreSQL) is reachable from the internet with no listener on instance	Informational	1
TCP port 544 (Kerberos) is reachable from the internet with no listener on instance	Informational	1
TCP port 546 (DHCP) is reachable from the internet with no listener on instance	Informational	1
TCP port 547 (DHCP) is reachable from the internet with no listener on instance	Informational	1
TCP port 601 (Syslog) is reachable from the internet with no listener on instance	Informational	1

TCP port 636 (LDAP over TLS) is reachable from the internet with no listener on instance	Informational	1
TCP port 67 (DHCP) is reachable from the internet with no listener on instance	Informational	1
TCP port 711 is reachable from the internet with active listener on instance	Low	1
TCP port 749 (Kerberos) is reachable from the internet with no listener on instance	Informational	1
TCP port 751 (Kerberos) is reachable from the internet with no listener on instance	Informational	1
TCP port 80 (HTTP) is reachable from the internet with no listener on instance	Informational	1
TCP port 88 (Kerberos) is reachable from the internet with no listener on instance	Informational	1
TCP port 9200 (Elasticsearch) is reachable from the internet with no listener on instance	Informational	1
TCP port 9300 (Elasticsearch) is reachable from the internet with no listener on instance	Informational	1
UDP port 111 (NFS) is reachable from the internet with active listener on instance	Informational	1
UDP port 111 (RPC) is reachable from the internet with active listener on instance	Informational	1
UDP port 1110 (NFS) is reachable from the internet with no listener on instance	Informational	1
UDP port 135 (RPC) is reachable from the internet with no listener on instance	Informational	1
UDP port 137 (NetBIOS) is reachable from the internet with no listener on instance	Informational	1
UDP port 138 (NetBIOS) is reachable from the internet with no listener on instance	Informational	1
UDP port 1434 (SQLServer) is reachable from the internet with no listener on instance	Informational	1
UDP port 1512 (WINS) is reachable from the internet with no listener on instance	Informational	1
UDP port 20 (FTP) is reachable from the internet with no listener on instance	Informational	1
UDP port 2049 (NFS) is reachable from the internet with no listener on instance	Informational	1
UDP port 21 (FTP) is reachable from the internet with no listener on instance	Informational	1
UDP port 23 (Telnet) is reachable from the internet with no listener on instance	Informational	1
UDP port 3389 (RDP) is reachable from the internet with no listener on instance	Informational	1

UDP port 4045 (NFS) is reachable from the internet with no listener on instance	Informational	1
UDP port 42 (WINS) is reachable from the internet with no listener on instance	Informational	1
UDP port 443 (HTTPS) is reachable from the internet with no listener on instance	Informational	1
UDP port 445 (SMB) is reachable from the internet with no listener on instance	Informational	1
UDP port 464 (Kerberos) is reachable from the internet with no listener on instance	Informational	1
UDP port 514 (Syslog) is reachable from the internet with no listener on instance	Informational	1
UDP port 515 (Print Services) is reachable from the internet with no listener on instance	Informational	1
UDP port 530 (RPC) is reachable from the internet with no listener on instance	Informational	1
UDP port 546 (DHCP) is reachable from the internet with no listener on instance	Informational	1
UDP port 547 (DHCP) is reachable from the internet with no listener on instance	Informational	1
UDP port 67 (DHCP) is reachable from the internet with no listener on instance	Informational	1
UDP port 68 (DHCP) is reachable from the internet with active listener on instance	Informational	1
UDP port 711 is reachable from the internet with active listener on instance	Low	1
UDP port 749 (Kerberos) is reachable from the internet with no listener on instance	Informational	1
UDP port 750 (Kerberos) is reachable from the internet with no listener on instance	Informational	1
UDP port 751 (Kerberos) is reachable from the internet with no listener on instance	Informational	1
UDP port 752 (Kerberos) is reachable from the internet with no listener on instance	Informational	1
UDP port 80 (HTTP) is reachable from the internet with no listener on instance	Informational	1
UDP port 88 (Kerberos) is reachable from the internet with no listener on instance	Informational	1

3.4: 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 - CIS Operating System Security Configuration Benchmarks-1.0

4.1.1 Level 1

1.1.2 Ensure /tmp is configured

Severity

High

Description

Description The /tmp directory is a world-writable directory used for temporary storage by all users and some applications. Rationale Making /tmp its own file system allows an administrator to set the noexec option on the mount, making /tmp useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system setuid program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw. This can be accomplished by either mounting tmpfs to /tmp, or creating a separate partition for /tmp.

Recommendation

Configure /etc/fstab as appropriate. example:tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0 or Run the following commands to enable systemd /tmp mounting: systemctl unmask tmp.mount systemctl enable tmp.mount Edit /etc/systemd/system/local-fs.target.wants/tmp.mount to configure the /tmp mount: [Mount]What=tmpfsWhere=/tmpType=tmpfsOptions=mode=1777,strictatime,noexec,nodev,nosuid Impact: Since the /tmp directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition. Running out of /tmp space is a

problem regardless of what kind of filesystem lies under it, but in a default installation a disk-based /tmp will essentially have the whole disk available, as it only creates a single / partition. On the other hand, a RAM-based /tmp as with tmpfs will almost certainly be much smaller, which can lead to applications filling up the filesystem much more easily./tmp utilizing tmpfs can be resized using the size={size} parameter on the Options line on the tmp.mount file

Failed Instances

i-079d0668bb45659b2

1.1.17 Ensure noexec option set on /dev/shm partition

Severity

High

Description

Description The noexec mount option specifies that the filesystem cannot contain executable binaries. Rationale Setting this option on a file system prevents users from executing programs from shared memory. This deters users from introducing potentially malicious software on the system.

Recommendation

Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /dev/shm partition. See the fstab(5) manual page for more information. Run the following command to remount /dev/shm : # mount -o remount,noexec /dev/shm

Failed Instances

i-079d0668bb45659b2

1.1.1.1 Ensure mounting of cramfs filesystems is disabled

Severity

High

Description

Description The cramfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A cramfs image can be used without having to first decompress the image. Rationale Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

Recommendation

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/cramfs.conf and add the following line: install cramfs /bin/true Run the following command to unload the cramfs module: # rmmod cramfs

Failed Instances

i-079d0668bb45659b2

1.1.1.2 Ensure mounting of hfs filesystems is disabled

Severity

High

Description

Description The hfs filesystem type is a hierarchical filesystem that allows you to mount Mac OS filesystems. **Rationale** Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/hfs.conf and add the following line: install hfs /bin/true Run the following command to unload the hfs module: # rmmod hfs

Failed Instances

i-079d0668bb45659b2

1.1.1.3 Ensure mounting of hfsplus filesystems is disabled

Severity

High

Description

Description The hfsplus filesystem type is a hierarchical filesystem designed to replace hfs that allows you to mount Mac OS filesystems. **Rationale** Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/ufsplus.conf and add the following line: install ufsplus /bin/true Run the following command to unload the ufsplus module: # rmmod ufsplus

Failed Instances

i-079d0668bb45659b2

1.1.1.4 Ensure mounting of squashfs filesystems is disabled

Severity

High

Description

Description The squashfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems (similar to cramfs). A squashfs image can be used without having to first decompress the image. Rationale Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/squashfs.conf and add the following line: install squashfs /bin/true Run the following command to unload the squashfs module: # rmmod squashfs

Failed Instances

i-079d0668bb45659b2

1.1.1.5 Ensure mounting of udf filesystems is disabled

Severity

High

Description

Description The udf filesystem type is the universal disk format used to implement ISO/IEC 13346 and ECMA-167 specifications. This is an open vendor filesystem type for data storage on a broad range of media. This filesystem type is necessary to support writing DVDs and newer optical disc formats. Rationale Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/udf.conf and add the following line: install udf /bin/true Run the following command to unload the udf module: # rmmod udf

Failed Instances

i-079d0668bb45659b2

1.3.1 Ensure AIDE is installed

Severity

High

Description

Description AIDE takes a snapshot of filesystem state including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system. Rationale By monitoring the filesystem state compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.

Recommendation

Run the following command to install aide : # yum install aide Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options.

Initialize AIDE: # aide --init# mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

Failed Instances

i-079d0668bb45659b2

1.3.2 Ensure filesystem integrity is regularly checked

Severity

High

Description

Description Periodic checking of the filesystem integrity is needed to detect changes to the filesystem. Rationale Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.

Recommendation

Run the following command: # crontab -u root -e Add the following line to the crontab:
0 5 * * * /usr/sbin/aide --check

Failed Instances

i-079d0668bb45659b2

1.5.1 Ensure core dumps are restricted

Severity

High

Description

Description A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file. The system provides the ability to set a soft limit for core dumps, but this can be overridden by the user. Rationale Setting a hard limit on core dumps prevents users from overriding the soft variable. If core dumps are required, consider setting limits for user groups (see limits.conf(5)). In addition, setting the fs.suid_dumpable variable to 0 will prevent setuid programs from dumping core.

Recommendation

Add the following line to /etc/security/limits.conf or a /etc/security/limits.d/* file:
* hard core 0 Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:
fs.suid_dumpable = 0 Run the following command to set the active kernel parameter: # sysctl -w fs.suid_dumpable=0

Failed Instances

i-079d0668bb45659b2

1.5.2 Ensure address space layout randomization (ASLR) is enabled

Severity

High

Description

Description Address space layout randomization (ASLR) is an exploit mitigation technique which randomly arranges the address space of key data areas of a process. Rationale Randomly placing virtual memory regions will make it difficult to write memory page exploits as the memory placement will be consistently shifting.

Recommendation

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:
kernel.randomize_va_space = 2 Run the following command to set the active kernel
parameter: # sysctl -w kernel.randomize_va_space=2

Failed Instances

i-079d0668bb45659b2

1.7.1.1 Ensure message of the day is configured properly

Severity

High

Description

Description The contents of the /etc/motd file are displayed to users after login and function as a message of the day for authenticated users. Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If mingetty(8) supports the following options, they display operating system information: \m - machine architecture \r - operating system release \s - operating system name \v - operating system version Rationale Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " uname -a " command once they have logged in.

Recommendation

Edit the /etc/motd file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s , \v. , or references to the OS platform

Failed Instances

i-079d0668bb45659b2

1.7.1.2 Ensure local login warning banner is configured properly

Severity

Informational

Description

Description The contents of the /etc/issue file are displayed to users prior to login for local terminals. Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If mingetty(8) supports the following options, they display operating system information: \m - machine architecture \r - operating system release \s - operating system name \v - operating system version Rationale Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " uname -a " command once they have logged in.

Recommendation

Edit the /etc/issue file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s , \v or references to the OS platform: # echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue

Failed Instances

i-079d0668bb45659b2

1.7.1.3 Ensure remote login warning banner is configured properly

Severity

Informational

Description

Description The contents of the /etc/issue.net file are displayed to users prior to login for remote connections from configured services. Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If mingetty(8) supports the following options, they display operating system information: \m - machine architecture \r - operating system release \s - operating system name \v - operating system version Rationale Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login

banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " uname -a " command once they have logged in.

Recommendation

Edit the /etc/issue.net file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s , or \v , or references to the OS platform: # echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue.net

Failed Instances

i-079d0668bb45659b2

3.1.1 Ensure IP forwarding is disabled

Severity

High

Description

Description The net.ipv4.ip_forward and net.ipv6.conf.all.forwarding flags are used to tell the system whether it can forward packets or not. Rationale Setting the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Recommendation

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:

net.ipv4.ip_forward = 0 net.ipv6.conf.all.forwarding = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.ip_forward=0# sysctl -w net.ipv6.conf.all.forwarding=0# sysctl -w net.ipv4.route.flush=1# sysctl -w net.ipv6.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.1.2 Ensure packet redirect sending is disabled

Severity

High

Description

Description ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects. **Rationale** An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.send_redirects = 0 net.ipv4.conf.default.send_redirects = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.send_redirects=0# sysctl -w net.ipv4.conf.default.send_redirects=0# sysctl -w net.ipv4.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.2.1 Ensure source routed packets are not accepted

Severity

High

Description

Description In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used. **Rationale** Setting net.ipv4.conf.all.accept_source_route, net.ipv4.conf.default.accept_source_route, net.ipv6.conf.all.accept_source_route and net.ipv6.conf.default.accept_source_route to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.accept_source_route = 0 net.ipv4.conf.default.accept_source_route = 0 net.ipv6.conf.all.accept_source_route = 0 net.ipv6.conf.default.accept_source_route = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.accept_source_route=0# sysctl -w net.ipv4.conf.default.accept_source_route=0# sysctl -w net.ipv6.conf.all.accept_source_route=0# sysctl -w net.ipv6.conf.default.accept_source_route=0# sysctl -w net.ipv4.route.flush=1# sysctl -w net.ipv6.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.2.2 Ensure ICMP redirects are not accepted

Severity

High

Description

Description ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.accept_redirects to 0, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables. Rationale Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0 net.ipv6.conf.all.accept_redirects = 0 net.ipv6.conf.default.accept_redirects = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.accept_redirects=0# sysctl -w net.ipv4.conf.default.accept_redirects=0# sysctl -w net.ipv6.conf.all.accept_redirects=0# sysctl -w net.ipv6.conf.default.accept_redirects=0# sysctl -w net.ipv4.route.flush=1# sysctl -w net.ipv6.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.2.3 Ensure secure ICMP redirects are not accepted

Severity

High

Description

Description Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure. Rationale It is still possible for even known gateways to be compromised. Setting net.ipv4.conf.all.secure_redirects to 0 protects the system from routing table updates by possibly compromised known gateways.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.secure_redirects = 0 net.ipv4.conf.default.secure_redirects = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.secure_redirects=0# sysctl -w net.ipv4.conf.default.secure_redirects=0# sysctl -w net.ipv4.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.2.4 Ensure suspicious packets are logged

Severity

High

Description

Description When enabled, this feature logs packets with un-routable source addresses to the kernel log. Rationale Enabling this feature and logging these packets allows an administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.log_martians = 1 net.ipv4.conf.default.log_martians = 1 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.log_martians=1# sysctl -w net.ipv4.conf.default.log_martians=1# sysctl -w net.ipv4.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.2.5 Ensure broadcast ICMP requests are ignored

Severity

High

Description

Description Setting net.ipv4.icmp_echo_ignore_broadcasts to 1 will cause the system to ignore all ICMP echo and timestamp requests to broadcast and multicast addresses. Rationale Accepting ICMP echo and timestamp requests with broadcast or multicast destinations for your network could be used to trick your host into starting (or participating) in a Smurf attack. A Smurf attack relies on an attacker sending large amounts of ICMP broadcast messages with a spoofed source address. All hosts receiving this message and responding would send echo-reply messages back to the spoofed address, which is probably not routable. If many hosts respond to the packets, the amount of traffic on the network could be significantly multiplied.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.icmp_echo_ignore_broadcasts = 1 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1# sysctl -w net.ipv4.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.2.6 Ensure bogus ICMP responses are ignored

Severity

High

Description

Description Setting icmp_ignore_bogus_error_responses to 1 prevents the kernel from logging bogus responses (RFC-1122 non-compliant) from broadcast reframes, keeping file systems from filling up with useless log messages. Rationale Some routers (and some attackers) will send responses that violate RFC-1122 and attempt to fill up a log file system with many useless error messages.

Recommendation

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.icmp_ignore_bogus_error_responses = 1 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1# sysctl -w net.ipv4.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.2.7 Ensure Reverse Path Filtering is enabled

Severity

High

Description

Description Setting net.ipv4.conf.all.rp_filter and net.ipv4.conf.default.rp_filter to 1 forces the Linux kernel to utilize reverse path filtering on a received packet to determine if the packet was valid. Essentially, with reverse path filtering, if the return packet does not go out the same interface that the corresponding source packet came from, the packet is dropped (and logged if log_martians is set). Rationale Setting these flags is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.rp_filter = 1 net.ipv4.conf.default.rp_filter = 1 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.rp_filter=1# sysctl -w net.ipv4.conf.default.rp_filter=1# sysctl -w net.ipv4.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.2.8 Ensure TCP SYN Cookies is enabled

Severity

High

Description

Description When `tcp_syncookies` is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue. **Rationale** Attackers use SYN flood attacks to perform a denial of service attacked on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. SYN cookies allow the system to keep accepting valid connections, even if under a denial of service attack.

Recommendation

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

`net.ipv4.tcp_syncookies = 1` Run the following commands to set the active kernel parameters: `# sysctl -w net.ipv4.tcp_syncookies=1# sysctl -w net.ipv4.route.flush=1`

Failed Instances

i-079d0668bb45659b2

3.2.9 Ensure IPv6 router advertisements are not accepted

Severity

High

Description

Description This setting disables the system's ability to accept IPv6 router advertisements. **Rationale** It is recommended that systems not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.

Recommendation

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

`net.ipv6.conf.all.accept_ra = 0``net.ipv6.conf.default.accept_ra = 0` Run the following commands to set the active kernel parameters: `# sysctl -w`

```
net.ipv6.conf.all.accept_ra=0# sysctl -w net.ipv6.conf.default.accept_ra=0# sysctl -w  
net.ipv6.route.flush=1
```

Failed Instances

i-079d0668bb45659b2

3.3.3 Ensure /etc/hosts.deny is configured

Severity

Informational

Description

Description The /etc/hosts.deny file specifies which IP addresses are not permitted to connect to the host. It is intended to be used in conjunction with the /etc/hosts.allow file.

Rationale The /etc/hosts.deny file serves as a failsafe so that any host not specified in /etc/hosts.allow is denied access to the system.

Recommendation

Run the following command to create /etc/hosts.deny : # echo "ALL: ALL" >> /etc/hosts.deny

Failed Instances

i-079d0668bb45659b2

3.4.1 Ensure DCCP is disabled

Severity

Informational

Description

Description The Datagram Congestion Control Protocol (DCCP) is a transport layer protocol that supports streaming media and telephony. DCCP provides a way to gain access to congestion control, without having to do it at the application layer, but does not provide in-sequence delivery. Rationale If the protocol is not required, it is recommended that the drivers not be installed to reduce the potential attack surface.

Recommendation

Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install dccp /bin/true

Failed Instances

i-079d0668bb45659b2

3.4.2 Ensure SCTP is disabled

Severity

Informational

Description

Description The Stream Control Transmission Protocol (SCTP) is a transport layer protocol used to support message oriented communication, with several streams of messages in one connection. It serves a similar function as TCP and UDP, incorporating features of both. It is message-oriented like UDP, and ensures reliable in-sequence transport of messages with congestion control like TCP. **Rationale** If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Recommendation

Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install sctp /bin/true

Failed Instances

i-079d0668bb45659b2

3.4.3 Ensure RDS is disabled

Severity

Informational

Description

Description The Reliable Datagram Sockets (RDS) protocol is a transport layer protocol designed to provide low-latency, high-bandwidth communications between cluster nodes. It was developed by the Oracle Corporation. **Rationale** If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Recommendation

Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install rds /bin/true

Failed Instances

i-079d0668bb45659b2

3.4.4 Ensure TIPC is disabled

Severity

Informational

Description

Description The Transparent Inter-Process Communication (TIPC) protocol is designed to provide communication between cluster nodes. Rationale If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Recommendation

Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install tipc /bin/true

Failed Instances

i-079d0668bb45659b2

3.5.1.1 Ensure default deny firewall policy

Severity

High

Description

Description A default deny all policy on connections ensures that any unconfigured network usage will be rejected. Rationale With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Recommendation

Run the following commands to implement a default DROP policy:
iptables -P INPUT DROP# iptables -P OUTPUT DROP# iptables -P FORWARD DROP

Failed Instances

i-079d0668bb45659b2

3.5.1.2 Ensure loopback traffic is configured

Severity

High

Description

Description Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8). Rationale Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Recommendation

Run the following commands to implement the loopback rules:
iptables -A INPUT -i lo -j ACCEPT# iptables -A OUTPUT -o lo -j ACCEPT# iptables -A INPUT -s 127.0.0.0/8 -j DROP

Failed Instances

i-079d0668bb45659b2

3.5.1.4 Ensure firewall rules exist for all open ports

Severity

High

Description

Description Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic. Rationale Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Recommendation

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections:
iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT

Failed Instances

i-079d0668bb45659b2

3.5.2.1 Ensure IPv6 default deny firewall policy

Severity

High

Description

Description A default deny all policy on connections ensures that any unconfigured network usage will be rejected. Rationale With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Recommendation

Run the following commands to implement a default DROP policy: # ip6tables -P INPUT DROP# ip6tables -P OUTPUT DROP# ip6tables -P FORWARD DROP

Failed Instances

i-079d0668bb45659b2

3.5.2.2 Ensure IPv6 loopback traffic is configured

Severity

High

Description

Description Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (>::1). Rationale Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (>::1) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Recommendation

Run the following commands to implement the loopback rules: # ip6tables -A INPUT -i lo -j ACCEPT# ip6tables -A OUTPUT -o lo -j ACCEPT# ip6tables -A INPUT -s ::1 -j DROP

Failed Instances

i-079d0668bb45659b2

4.2.4 Ensure permissions on all logfiles are configured

Severity

High

Description

Description Log files stored in /var/log/ contain logged information from many services on the system, or on log hosts others as well. Rationale It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Recommendation

Run the following command to set permissions on all existing log files: # find -L /var/log -type f -exec chmod g-wx,o-rwx {} +

Failed Instances

i-079d0668bb45659b2

4.2.1.3 Ensure rsyslog default file permissions configured

Severity

High

Description

Description rsyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files. Rationale It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Recommendation

Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and set \$FileCreateMode to 0640 or more restrictive: \$FileCreateMode 0640

Failed Instances

i-079d0668bb45659b2

4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host

Severity

High

Description

Description The rsyslog utility supports the ability to send logs it gathers to a remote log host running syslogd(8) or to receive messages from remote hosts, reducing administrative overhead. Rationale Storing log data on a remote host protects log

integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system

Recommendation

Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and add the following line (where loghost.example.com is the name of your central log host). *.*

@@loghost.example.com Run the following command to reload the rsyslogd configuration: # pkill -HUP rsyslogd

Failed Instances

i-079d0668bb45659b2

5.6 Ensure access to the su command is restricted

Severity

High

Description

Description The su command allows a user to run a command or shell as another user. The program has been superseded by sudo , which allows for more granular control over privileged access. Normally, the su command can be executed by any user. By uncommenting the pam_wheel.so statement in /etc/pam.d/su , the su command will only allow users in the wheel group to execute su . Rationale Restricting the use of su , and using sudo in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The sudo utility also provides a better logging and audit mechanism, as it can log each command executed via sudo , whereas su can only record that a user executed the su program.

Recommendation

Add the following line to the /etc/pam.d/su file: auth required pam_wheel.so use_uid Create a comma separated list of users in the wheel statement in the /etc/group file: wheel:x:10:<user list>

Failed Instances

i-079d0668bb45659b2

5.1.2 Ensure permissions on /etc/crontab are configured

Severity

High

Description

Description The /etc/crontab file is used by cron to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file. **Rationale** This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Recommendation

Run the following commands to set ownership and permissions on /etc/crontab : # chown root:root /etc/crontab# chmod og-rwx /etc/crontab

Failed Instances

i-079d0668bb45659b2

5.1.3 Ensure permissions on /etc/cron.hourly are configured

Severity

High

Description

Description This directory contains system cron jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. **Rationale** Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation

Run the following commands to set ownership and permissions on /etc/cron.hourly : # chown root:root /etc/cron.hourly# chmod og-rwx /etc/cron.hourly

Failed Instances

i-079d0668bb45659b2

5.1.4 Ensure permissions on /etc/cron.daily are configured

Severity

High

Description

Description The /etc/cron.daily directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation

Run the following commands to set ownership and permissions on /etc/cron.daily : # chown root:root /etc/cron.daily# chmod og-rwx /etc/cron.daily

Failed Instances

i-079d0668bb45659b2

5.1.5 Ensure permissions on /etc/cron.weekly are configured

Severity

High

Description

Description The /etc/cron.weekly directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation

Run the following commands to set ownership and permissions on /etc/cron.weekly : # chown root:root /etc/cron.weekly# chmod og-rwx /etc/cron.weekly

Failed Instances

i-079d0668bb45659b2

5.1.6 Ensure permissions on /etc/cron.monthly are configured

Severity

High

Description

Description The /etc/cron.monthly directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation

Run the following commands to set ownership and permissions on /etc/cron.monthly : # chown root:root /etc/cron.monthly# chmod og-rwx /etc/cron.monthly

Failed Instances

i-079d0668bb45659b2

5.1.7 Ensure permissions on /etc/cron.d are configured

Severity

High

Description

Description The /etc/cron.d directory contains system cron jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from /etc/crontab , but require more granular control as to when they run. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them

the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation

Run the following commands to set ownership and permissions on /etc/cron.d : # chown root:root /etc/cron.d# chmod og-rwx /etc/cron.d

Failed Instances

i-079d0668bb45659b2

5.1.8 Ensure at/cron is restricted to authorized users

Severity

High

Description

Description Configure /etc/cron.allow and /etc/at.allow to allow specific users to use these services. If /etc/cron.allow or /etc/at.allow do not exist, then /etc/at.deny and /etc/cron.deny are checked. Any user not specifically defined in those files is allowed to use at and cron. By removing the files, only users in /etc/cron.allow and /etc/at.allow are allowed to use at and cron. Note that even though a given user is not listed in cron.allow , cron jobs can still be run as that user. The cron.allow file only controls administrative access to the crontab command for scheduling and modifying cron jobs.

Rationale On many systems, only the system administrator is authorized to schedule cron jobs. Using the cron.allow file to control who can run cron jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Recommendation

Run the following commands to remove /etc/cron.deny and /etc/at.deny and create and set permissions and ownership for /etc/cron.allow and /etc/at.allow : # rm /etc/cron.deny# rm /etc/at.deny# touch /etc/cron.allow# touch /etc/at.allow# chmod og-rwx /etc/cron.allow# chmod og-rwx /etc/at.allow# chown root:root /etc/cron.allow# chown root:root /etc/at.allow

Failed Instances

i-079d0668bb45659b2

5.2.4 Ensure SSH Protocol is set to 2

Severity

High

Description

Description SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. SSH2 is more advanced and secure. Rationale SSH v1 suffers from insecurities that do not affect SSH v2.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows: Protocol 2

Failed Instances

i-079d0668bb45659b2

5.2.5 Ensure SSH LogLevel is appropriate

Severity

High

Description

Description INFO level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field. VERBOSE level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments. Rationale SSH provides several logging levels with varying amounts of verbosity. DEBUG is specifically not recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows: LogLevel VERBOSE or LogLevel INFO

Failed Instances

i-079d0668bb45659b2

5.2.7 Ensure SSH MaxAuthTries is set to 4 or less

Severity

High

Description

Description The MaxAuthTries parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the syslog file detailing the login failure. Rationale Setting the MaxAuthTries parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows: MaxAuthTries 4

Failed Instances

i-079d0668bb45659b2

5.2.8 Ensure SSH IgnoreRhosts is enabled

Severity

High

Description

Description The IgnoreRhosts parameter specifies that .rhosts and .shosts files will not be used in RhostsRSAAuthentication or HostbasedAuthentication . Rationale Setting this parameter forces users to enter a password when authenticating with ssh.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows: IgnoreRhosts yes

Failed Instances

i-079d0668bb45659b2

5.2.9 Ensure SSH HostbasedAuthentication is disabled

Severity

High

Description

Description The HostbasedAuthentication parameter specifies if authentication is allowed through trusted hosts via the user of `.rhosts` , or `/etc/hosts.equiv` , along with successful public key client host authentication. This option only applies to SSH Protocol Version 2. **Rationale** Even though the `.rhosts` files are ineffective if support is disabled in `/etc/pam.conf` , disabling the ability to use `.rhosts` files in SSH provides an additional layer of protection .

Recommendation

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows:

`HostbasedAuthentication no`

Failed Instances

i-079d0668bb45659b2

5.2.10 Ensure SSH root login is disabled

Severity

High

Description

Description The PermitRootLogin parameter specifies if the root user can log in using `ssh(1)`. The default is no. **Rationale** Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root via `sudo` or `su` . This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident

Recommendation

Edit the `/etc/ssh/sshd_config` file to set the parameter as follows: `PermitRootLogin no`

Failed Instances

i-079d0668bb45659b2

5.2.11 Ensure SSH PermitEmptyPasswords is disabled

Severity

High

Description

Description The PermitEmptyPasswords parameter specifies if the SSH server allows login to accounts with empty password strings. **Rationale** Disallowing remote shell

access to accounts that have an empty password reduces the probability of unauthorized access to the system

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

PermitEmptyPasswords no

Failed Instances

i-079d0668bb45659b2

5.2.12 Ensure SSH PermitUserEnvironment is disabled

Severity

High

Description

Description The PermitUserEnvironment option allows users to present environment options to the ssh daemon. Rationale Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has ssh executing trojan'd programs)

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

PermitUserEnvironment no

Failed Instances

i-079d0668bb45659b2

5.2.13 Ensure only strong ciphers are used

Severity

High

Description

Description This variable limits the ciphers that SSH can use during communication. Rationale Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised The DES, Triple DES, and Blowfish ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration

encrypted session, aka a "Sweet32" attack. The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue. The passwords used during an SSH session encrypted with RC4 can be recovered by an attacker who is able to capture and replay the session Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors. The `mm_newkeys_from_blob` function in `monitor_wrap.c`, when an AES-GCM cipher is used, does not properly initialize memory for a MAC context data structure, which allows remote authenticated users to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address.

Recommendation

Edit the `/etc/ssh/sshd_config` file add/modify the `Ciphers` line to contain a comma separated list of the site approved ciphers Example: `Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr`

Failed Instances

i-079d0668bb45659b2

5.2.14 Ensure only strong MAC algorithms are used

Severity

High

Description

Description This variable limits the types of MAC algorithms that SSH can use during communication. **Rationale** MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information.

Recommendation

Edit the /etc/ssh/sshd_config file and add/modify the MACs line to contain a comma separated list of the site approved MACs Example: MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256

Failed Instances

i-079d0668bb45659b2

5.2.15 Ensure that strong Key Exchange algorithms are used

Severity

High

Description

Description Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received Rationale Key exchange methods that are considered weak should be removed. A key exchange method may be weak because too few bits are used, or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

Recommendation

Edit the /etc/ssh/sshd_config file add/modify the KexAlgorithms line to contain a comma separated list of the site approved key exchange algorithms Example: KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp251,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256

Failed Instances

i-079d0668bb45659b2

5.2.16 Ensure SSH Idle Timeout Interval is configured

Severity

High

Description

Description The two options ClientAliveInterval and ClientAliveCountMax control the timeout of ssh sessions. When the ClientAliveInterval variable is set, ssh sessions

that have no activity for the specified length of time are terminated. When the ClientAliveCountMax variable is set, sshd will send client alive messages at every ClientAliveInterval interval. When the number of consecutive client alive messages are sent with no response from the client, the ssh session is terminated. For example, if the ClientAliveInterval is set to 15 seconds and the ClientAliveCountMax is set to 3, the client ssh session will be terminated after 45 seconds of idle time. Rationale Having no timeout value associated with a connection could allow an unauthorized user access to another user's ssh session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening.. While the recommended setting is 300 seconds (5 minutes), set this timeout value based on site policy. The recommended setting for ClientAliveCountMax is 0. In this case, the client session will be terminated after 5 minutes of idle time and no keepalive messages will be sent.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameters according to site policy:
ClientAliveInterval 300ClientAliveCountMax 0

Failed Instances

i-079d0668bb45659b2

5.2.17 Ensure SSH LoginGraceTime is set to one minute or less

Severity

High

Description

Description The LoginGraceTime parameter specifies the time allowed for successful authentication to the SSH server. The longer the Grace period is the more open unauthenticated connections can exist. Like other session controls in this session the Grace Period should be limited to appropriate organizational limits to ensure the service is available for needed access. Rationale Setting the LoginGraceTime parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. It will also limit the number of concurrent unauthenticated connections While the recommended setting is 60 seconds (1 Minute), set the number based on site policy.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows: LoginGraceTime 60

Failed Instances

i-079d0668bb45659b2

5.2.18 Ensure SSH access is limited

Severity

High

Description

Description There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged: AllowUsers The AllowUsers variable gives the system administrator the option of allowing specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host. AllowGroups The AllowGroups variable gives the system administrator the option of allowing specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable. DenyUsers The DenyUsers variable gives the system administrator the option of denying specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host. DenyGroups The DenyGroups variable gives the system administrator the option of denying specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable. Rationale Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Recommendation

Edit the /etc/ssh/sshd_config file to set one or more of the parameter as follows:
AllowUsers <userlist>AllowGroups <grouplist>DenyUsers <userlist>DenyGroups <grouplist>

Failed Instances

i-079d0668bb45659b2

5.2.19 Ensure SSH warning banner is configured

Severity

High

Description

Description The Banner parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed.

Rationale Banners are used to warn connecting users of the particular site's policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows: Banner /etc/issue.net

Failed Instances

i-079d0668bb45659b2

5.3.1 Ensure password creation requirements are configured

Severity

High

Description

Description The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more. The following are definitions of the pam_pwquality .so options. try_first_pass - retrieve the password from a previous stacked PAM module. If not available, then prompt the user for a password.retry=3 - Allow 3 tries before sending back a failure. The following options are set in the /etc/security/pwquality.conf file: minlen = 14 - password must be 14 characters or morecredit = -1 - provide at least one digitcredit = -1 - provide at least one uppercase charactercredit = -1 - provide at least one lowercase character The settings shown above are one possible policy. Alter these values to conform to your own organization's password policies.

Rationale Strong passwords protect systems from being hacked through brute force methods.

Recommendation

Edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files to include the appropriate options for pam_pwquality.so and to conform to site policy: password requisite pam_pwquality.so try_first_pass retry=3 Edit /etc/security/pwquality.conf to add or update the following settings to conform to site policy: minlen = 14dcredit = -1ucredit = -1ocredit = -1lcredit = -1

Failed Instances

i-079d0668bb45659b2

5.3.2 Ensure lockout for failed password attempts is configured

Severity

High

Description

Description Lock out users after n unsuccessful consecutive login attempts. The first sets of changes are made to the PAM configuration files. The second set of changes are applied to the program specific PAM configuration file. The second set of changes must be applied to each program that will lock out users. Check the documentation for each secondary program for instructions on how to configure them to work with PAM. Set the lockout number to the policy in effect at your site. Rationale Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Recommendation

Edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files and add the following pam_faillock.so lines surrounding a pam_unix.so line modify the pam_unix.so is [success=1 default=bad] as listed in both: auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900auth [success=1 default=bad] pam_unix.so auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900

Failed Instances

i-079d0668bb45659b2

5.3.3 Ensure password reuse is limited

Severity

High

Description

Description The /etc/security/opasswd file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords. Rationale Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password. Note that these changes only apply to accounts configured on the local system.

Recommendation

Edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files to include the remember option and conform to site policy as shown: password sufficient pam_unix.so remember=5 or password required pam_pwhistory.so remember=5

Failed Instances

i-079d0668bb45659b2

5.4.4 Ensure default user umask is 027 or more restrictive

Severity

High

Description

Description The default umask determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the chmod command. Users who wish to allow their files and directories to be readable by others by default may choose a different default umask by inserting the umask command into the standard shell configuration files (.profile , .bashrc , etc.) in their home directories. Rationale Setting a very secure default value for umask ensures that users make a conscious choice about their file permissions. A default umask setting of 077 causes files and directories created by users to not be readable by any other user on the system. A umask of 027 would make files and directories readable by users in the same Unix group, while a umask of 022 would make files readable by every user on the system.

Recommendation

Edit the /etc/bashrc, /etc/profile and /etc/profile.d/* .sh files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows: umask 027

Failed Instances

i-079d0668bb45659b2

5.4.1.1 Ensure password expiration is 365 days or less

Severity

High

Description

Description The PASS_MAX_DAYS parameter in /etc/login.defs allows an administrator to force passwords to expire once they reach a defined age. It is recommended that the PASS_MAX_DAYS parameter be set to less than or equal to 365 days. Rationale The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity.

Recommendation

Set the PASS_MAX_DAYS parameter to conform to site policy in /etc/login.defs :
PASS_MAX_DAYS 90 Modify user parameters for all users with a password set to match: # chage --maxdays 90 <user>

Failed Instances

i-079d0668bb45659b2

5.4.1.2 Ensure minimum days between password changes is 7 or more

Severity

High

Description

Description The PASS_MIN_DAYS parameter in /etc/login.defs allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that PASS_MIN_DAYS parameter be set to 7 or more days. Rationale By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Recommendation

Set the PASS_MIN_DAYS parameter to 7 in /etc/login.defs : PASS_MIN_DAYS 7
Modify user parameters for all users with a password set to match: # chage --mindays 7 <user>

Failed Instances

i-079d0668bb45659b2

5.4.1.4 Ensure inactive password lock is 30 days or less

Severity

High

Description

Description User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled. Rationale Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Recommendation

Run the following command to set the default password inactivity period to 30 days: # useradd -D -f 30 Modify user parameters for all users with a password set to match: # chage --inactive 30 <user>

Failed Instances

i-079d0668bb45659b2

4.1.2 Level 2

1.1.2 Ensure /tmp is configured

Severity

High

Description

Description The /tmp directory is a world-writable directory used for temporary storage by all users and some applications. Rationale Making /tmp its own file system allows an administrator to set the noexec option on the mount, making /tmp useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system setuid program and wait for it to be updated. Once the program was

updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw. This can be accomplished by either mounting tmpfs to /tmp, or creating a separate partition for /tmp.

Recommendation

Configure /etc/fstab as appropriate. example:tmpfs /tmp tmpfs defaults,rw,nosuid,nodev,noexec,relatime 0 0 or Run the following commands to enable systemd /tmp mounting: systemctl unmask tmp.mountsystemctl enable tmp.mount Edit /etc/systemd/system/local-fs.target.wants/tmp.mount to configure the /tmp mount: [Mount]What=tmpfsWhere=/tmpType=tmpfsOptions=mode=1777,strictatime,noexec,nodev,nosuid Impact: Since the /tmp directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition.Running out of /tmp space is a problem regardless of what kind of filesystem lies under it, but in a default installation a disk-based /tmp will essentially have the whole disk available, as it only creates a single / partition. On the other hand, a RAM-based /tmp as with tmpfs will almost certainly be much smaller, which can lead to applications filling up the filesystem much more easily./tmp utalizing tmpfs can be resized using the size={size} parameter on the Options line on the tmp.mount file

Failed Instances

i-079d0668bb45659b2

1.1.6 Ensure separate partition exists for /var

Severity

High

Description

Description The /var directory is used by daemons and other system services to temporarily store dynamic data. Some directories created by these processes may be world-writable. Rationale Since the /var directory may contain world-writable files and directories, there is a risk of resource exhaustion if it is not bound to a separate partition.

Recommendation

For new installations, during installation create a custom partition setup and specify a separate partition for /var . For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate. Impact: Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent

successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Failed Instances

i-079d0668bb45659b2

1.1.7 Ensure separate partition exists for /var/tmp

Severity

High

Description

Description The /var/tmp directory is a world-writable directory used for temporary storage by all users and some applications. **Rationale** Since the /var/tmp directory is intended to be world-writable, there is a risk of resource exhaustion if it is not bound to a separate partition. In addition, making /var/tmp its own file system allows an administrator to set the noexec option on the mount, making /var/tmp useless for an attacker to install executable code. It would also prevent an attacker from establishing a hardlink to a system setuid program and wait for it to be updated. Once the program was updated, the hardlink would be broken and the attacker would have his own copy of the program. If the program happened to have a security vulnerability, the attacker could continue to exploit the known flaw.

Recommendation

For new installations, during installation create a custom partition setup and specify a separate partition for /var/tmp. For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate. **Impact:** Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Failed Instances

i-079d0668bb45659b2

1.1.11 Ensure separate partition exists for /var/log

Severity

High

Description

Description The /var/log directory is used by system services to store log data .

Rationale There are two important reasons to ensure that system logs are stored on a separate partition: protection against resource exhaustion (since logs can grow quite large) and protection of audit data.

Recommendation

For new installations, during installation create a custom partition setup and specify a separate partition for /var/log . For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate. Impact: Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Failed Instances

i-079d0668bb45659b2

1.1.12 Ensure separate partition exists for /var/log/audit

Severity

High

Description

Description The auditing daemon, auditd , stores log data in the /var/log/audit directory.

Rationale There are two important reasons to ensure that data gathered by auditd is stored on a separate partition: protection against resource exhaustion (since the audit.log file can grow quite large) and protection of audit data. The audit daemon calculates how much free space is left and performs actions based on the results. If other processes (such as syslog) consume space in the same partition as auditd , it may not perform as desired.

Recommendation

For new installations, during installation create a custom partition setup and specify a separate partition for /var/log/audit . For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate. Impact: Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent

successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Failed Instances

i-079d0668bb45659b2

1.1.13 Ensure separate partition exists for /home

Severity

High

Description

Description The /home directory is used to support disk storage needs of local users.

Rationale If the system is intended to support local users, create a separate partition for the /home directory to protect against resource exhaustion and restrict the type of files that can be stored under /home .

Recommendation

For new installations, during installation create a custom partition setup and specify a separate partition for /home . For systems that were previously installed, create a new partition and configure /etc/fstab as appropriate. Impact: Resizing filesystems is a common activity in cloud-hosted servers. Separate filesystem partitions may prevent successful resizing, or may require the installation of additional tools solely for the purpose of resizing operations. The use of these additional tools may introduce their own security considerations.

Failed Instances

i-079d0668bb45659b2

1.1.17 Ensure noexec option set on /dev/shm partition

Severity

High

Description

Description The noexec mount option specifies that the filesystem cannot contain executable binaries. Rationale Setting this option on a file system prevents users from executing programs from shared memory. This deters users from introducing potentially malicious software on the system.

Recommendation

Edit the /etc/fstab file and add noexec to the fourth field (mounting options) for the /dev/shm partition. See the fstab(5) manual page for more information. Run the following command to remount /dev/shm : # mount -o remount,noexec /dev/shm

Failed Instances

i-079d0668bb45659b2

1.1.1.1 Ensure mounting of cramfs filesystems is disabled

Severity

High

Description

Description The cramfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems. A cramfs image can be used without having to first decompress the image. **Rationale** Removing support for unneeded filesystem types reduces the local attack surface of the server. If this filesystem type is not needed, disable it.

Recommendation

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/cramfs.conf and add the following line: install cramfs /bin/true Run the following command to unload the cramfs module: # rmmod cramfs

Failed Instances

i-079d0668bb45659b2

1.1.1.2 Ensure mounting of hfs filesystems is disabled

Severity

High

Description

Description The hfs filesystem type is a hierarchical filesystem that allows you to mount Mac OS filesystems. **Rationale** Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/hfs.conf and add the following line: install hfs /bin/true Run the following command to unload the hfs module: # rmmod hfs

Failed Instances

i-079d0668bb45659b2

1.1.1.3 Ensure mounting of hfsplus filesystems is disabled

Severity

High

Description

Description The hfsplus filesystem type is a hierarchical filesystem designed to replace hfs that allows you to mount Mac OS filesystems. Rationale Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/hfsplus.conf and add the following line: install hfsplus /bin/true Run the following command to unload the hfsplus module: # rmmod hfsplus

Failed Instances

i-079d0668bb45659b2

1.1.1.4 Ensure mounting of squashfs filesystems is disabled

Severity

High

Description

Description The squashfs filesystem type is a compressed read-only Linux filesystem embedded in small footprint systems (similar to cramfs). A squashfs image can be used without having to first decompress the image. Rationale Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/squashfs.conf and add the following line: install squashfs /bin/true Run the following command to unload the squashfs module: # rmmod squashfs

Failed Instances

i-079d0668bb45659b2

1.1.1.5 Ensure mounting of udf filesystems is disabled

Severity

High

Description

Description The udf filesystem type is the universal disk format used to implement ISO/IEC 13346 and ECMA-167 specifications. This is an open vendor filesystem type for data storage on a broad range of media. This filesystem type is necessary to support writing DVDs and newer optical disc formats. Rationale Removing support for unneeded filesystem types reduces the local attack surface of the system. If this filesystem type is not needed, disable it.

Recommendation

Edit or create a file in the /etc/modprobe.d/ directory ending in .conf Example: vim /etc/modprobe.d/udf.conf and add the following line: install udf /bin/true Run the following command to unload the udf module: # rmmod udf

Failed Instances

i-079d0668bb45659b2

1.3.1 Ensure AIDE is installed

Severity

High

Description

Description AIDE takes a snapshot of filesystem state including modification times, permissions, and file hashes which can then be used to compare against the current state of the filesystem to detect modifications to the system. Rationale By monitoring the filesystem state compromised files can be detected to prevent or limit the exposure of accidental or malicious misconfigurations or modified binaries.

Recommendation

Run the following command to install aide : # yum install aide Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options.

Initialize AIDE: # aide --init# mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz

Failed Instances

i-079d0668bb45659b2

1.3.2 Ensure filesystem integrity is regularly checked

Severity

High

Description

Description Periodic checking of the filesystem integrity is needed to detect changes to the filesystem. Rationale Periodic file checking allows the system administrator to determine on a regular basis if critical files have been changed in an unauthorized fashion.

Recommendation

Run the following command: # crontab -u root -e Add the following line to the crontab:
0 5 * * * /usr/sbin/aide --check

Failed Instances

i-079d0668bb45659b2

1.5.1 Ensure core dumps are restricted

Severity

High

Description

Description A core dump is the memory of an executable program. It is generally used to determine why a program aborted. It can also be used to glean confidential information from a core file. The system provides the ability to set a soft limit for core dumps, but this can be overridden by the user. Rationale Setting a hard limit on core dumps prevents users from overriding the soft variable. If core dumps are required, consider setting limits for user groups (see limits.conf(5)). In addition, setting the fs.suid_dumpable variable to 0 will prevent setuid programs from dumping core.

Recommendation

Add the following line to /etc/security/limits.conf or a /etc/security/limits.d/* file:
* hard core 0 Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:
fs.suid_dumpable = 0 Run the following command to set the active kernel parameter: # sysctl -w fs.suid_dumpable=0

Failed Instances

i-079d0668bb45659b2

1.5.2 Ensure address space layout randomization (ASLR) is enabled

Severity

High

Description

Description Address space layout randomization (ASLR) is an exploit mitigation technique which randomly arranges the address space of key data areas of a process.
Rationale Randomly placing virtual memory regions will make it difficult to write memory page exploits as the memory placement will be consistently shifting.

Recommendation

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:
kernel.randomize_va_space = 2 Run the following command to set the active kernel parameter: # sysctl -w kernel.randomize_va_space=2

Failed Instances

i-079d0668bb45659b2

1.6.1.2 Ensure the SELinux state is enforcing

Severity

High

Description

Description Set SELinux to enable when the system is booted. Rationale SELinux must be enabled at boot time in to ensure that the controls it provides are in effect at all times.

Recommendation

Edit the /etc/selinux/config file to set the SELINUX parameter: SELINUX=enforcing

Failed Instances

i-079d0668bb45659b2

1.6.1.3 Ensure SELinux policy is configured

Severity

High

Description

Description Configure SELinux to meet or exceed the default targeted policy, which constrains daemons and system software only. Rationale Security configuration requirements vary from site to site. Some sites may mandate a policy that is stricter than the default policy, which is perfectly acceptable. This item is intended to ensure that at least the default recommendations are met.

Recommendation

Edit the /etc/selinux/config file to set the SELINUXTYPE parameter:
SELINUXTYPE=targeted

Failed Instances

i-079d0668bb45659b2

1.6.1.6 Ensure no unconfined daemons exist

Severity

High

Description

Description Daemons that are not defined in SELinux policy will inherit the security context of their parent process. Rationale Since daemons are launched and descend from the init process, they will inherit the security context label initrc_t . This could cause the unintended consequence of giving the process more permission than it requires.

Recommendation

Investigate any unconfined daemons found during the audit action. They may need to have an existing security context assigned to them or a policy built for them.

Failed Instances

i-079d0668bb45659b2

1.7.1.1 Ensure message of the day is configured properly

Severity

High

Description

Description The contents of the /etc/motd file are displayed to users after login and function as a message of the day for authenticated users. Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If mingetty(8) supports the following options, they display operating system information: \m - machine architecture \r - operating system release \s - operating system name \v - operating system version Rationale Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " uname -a " command once they have logged in.

Recommendation

Edit the /etc/motd file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s ,\v. , or references to the OS platform

Failed Instances

i-079d0668bb45659b2

1.7.1.2 Ensure local login warning banner is configured properly

Severity

Informational

Description

Description The contents of the /etc/issue file are displayed to users prior to login for local terminals. Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If mingetty(8) supports the following options, they display operating system information: \m - machine architecture \r - operating system release \s - operating system name \v - operating system version Rationale Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of

the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " uname -a " command once they have logged in.

Recommendation

Edit the /etc/issue file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s , \v or references to the OS platform: # echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue

Failed Instances

i-079d0668bb45659b2

1.7.1.3 Ensure remote login warning banner is configured properly

Severity

Informational

Description

Description The contents of the /etc/issue.net file are displayed to users prior to login for remote connections from configured services. Unix-based systems have typically displayed information about the OS release and patch level upon logging in to the system. This information can be useful to developers who are developing software for a particular OS platform. If mingetty(8) supports the following options, they display operating system information: \m - machine architecture \r - operating system release \s - operating system name \v - operating system version Rationale Warning messages inform users who are attempting to login to the system of their legal status regarding the system and must include the name of the organization that owns the system and any monitoring policies that are in place. Displaying OS and patch level information in login banners also has the side effect of providing detailed system information to attackers attempting to target specific exploits of a system. Authorized users can easily get this information by running the " uname -a " command once they have logged in.

Recommendation

Edit the /etc/issue.net file with the appropriate contents according to your site policy, remove any instances of \m , \r , \s , or \v , or references to the OS platform: # echo "Authorized uses only. All activity may be monitored and reported." > /etc/issue.net

Failed Instances

i-079d0668bb45659b2

3.6 Disable IPv6

Severity

Informational

Description

Description Although IPv6 has many advantages over IPv4, not all organizations have IPv6 or dual stack configurations implemented. Rationale If IPv6 or dual stack is not to be used, it is recommended that IPv6 be disabled to reduce the attack surface of the system.

Recommendation

Edit /etc/default/grub and remove add ipv6.disable=1 to the GRUB_CMDLINE_LINUX parameters: GRUB_CMDLINE_LINUX="ipv6.disable=1" Run the following command to update the grub2 configuration: # grub2-mkconfig -o /boot/grub2/grub.cfg

Failed Instances

i-079d0668bb45659b2

3.1.1 Ensure IP forwarding is disabled

Severity

High

Description

Description The net.ipv4.ip_forward and net.ipv6.conf.all.forwarding flags are used to tell the system whether it can forward packets or not. Rationale Setting the flags to 0 ensures that a system with multiple interfaces (for example, a hard proxy), will never be able to forward packets, and therefore, never serve as a router.

Recommendation

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file:
net.ipv4.ip_forward = 0 net.ipv6.conf.all.forwarding = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.ip_forward=0# sysctl -w net.ipv6.conf.all.forwarding=0# sysctl -w net.ipv4.route.flush=1# sysctl -w net.ipv6.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.1.2 Ensure packet redirect sending is disabled

Severity

High

Description

Description ICMP Redirects are used to send routing information to other hosts. As a host itself does not act as a router (in a host only configuration), there is no need to send redirects. Rationale An attacker could use a compromised host to send invalid ICMP redirects to other router devices in an attempt to corrupt routing and have users access a system set up by the attacker as opposed to a valid system.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.send_redirects = 0 net.ipv4.conf.default.send_redirects = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.send_redirects=0# sysctl -w net.ipv4.conf.default.send_redirects=0# sysctl -w net.ipv4.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.2.1 Ensure source routed packets are not accepted

Severity

High

Description

Description In networking, source routing allows a sender to partially or fully specify the route packets take through a network. In contrast, non-source routed packets travel a path determined by routers in the network. In some cases, systems may not be routable or reachable from some locations (e.g. private addresses vs. Internet routable), and so source routed packets would need to be used. Rationale Setting net.ipv4.conf.all.accept_source_route, net.ipv4.conf.default.accept_source_route, net.ipv6.conf.all.accept_source_route and net.ipv6.conf.default.accept_source_route to 0 disables the system from accepting source routed packets. Assume this system was capable of routing packets to

Internet routable addresses on one interface and private addresses on another interface. Assume that the private addresses were not routable to the Internet routable addresses and vice versa. Under normal routing circumstances, an attacker from the Internet routable addresses could not use the system as a way to reach the private address systems. If, however, source routed packets were allowed, they could be used to gain access to the private address systems as the route could be specified, rather than rely on routing protocols that did not allow this routing.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.accept_source_route = 0 net.ipv4.conf.default.accept_source_route = 0 net.ipv6.conf.all.accept_source_route = 0 net.ipv6.conf.default.accept_source_route = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.accept_source_route=0# sysctl -w net.ipv4.conf.default.accept_source_route=0# sysctl -w net.ipv6.conf.all.accept_source_route=0# sysctl -w net.ipv6.conf.default.accept_source_route=0# sysctl -w net.ipv4.route.flush=1# sysctl -w net.ipv6.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.2.2 Ensure ICMP redirects are not accepted

Severity

High

Description

Description ICMP redirect messages are packets that convey routing information and tell your host (acting as a router) to send packets via an alternate path. It is a way of allowing an outside routing device to update your system routing tables. By setting net.ipv4.conf.all.accept_redirects and net.ipv6.conf.all.accept_redirects to 0, the system will not accept any ICMP redirect messages, and therefore, won't allow outsiders to update the system's routing tables. Rationale Attackers could use bogus ICMP redirect messages to maliciously alter the system routing tables and get them to send packets to incorrect networks and allow your system packets to be captured.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.accept_redirects = 0 net.ipv4.conf.default.accept_redirects = 0 net.ipv6.conf.all.accept_redirects = 0 net.ipv6.conf.default.accept_redirects = 0 Run the following

commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.accept_redirects=0# sysctl -w net.ipv4.conf.default.accept_redirects=0# sysctl -w net.ipv6.conf.all.accept_redirects=0# sysctl -w net.ipv6.conf.default.accept_redirects=0# sysctl -w net.ipv4.route.flush=1# sysctl -w net.ipv6.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.2.3 Ensure secure ICMP redirects are not accepted

Severity

High

Description

Description Secure ICMP redirects are the same as ICMP redirects, except they come from gateways listed on the default gateway list. It is assumed that these gateways are known to your system, and that they are likely to be secure. Rationale It is still possible for even known gateways to be compromised. Setting net.ipv4.conf.all.secure_redirects to 0 protects the system from routing table updates by possibly compromised known gateways.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.secure_redirects = 0net.ipv4.conf.default.secure_redirects = 0 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.secure_redirects=0# sysctl -w net.ipv4.conf.default.secure_redirects=0# sysctl -w net.ipv4.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.2.4 Ensure suspicious packets are logged

Severity

High

Description

Description When enabled, this feature logs packets with un-routable source addresses to the kernel log. Rationale Enabling this feature and logging these packets allows an

administrator to investigate the possibility that an attacker is sending spoofed packets to their system.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:

net.ipv4.conf.all.log_martians = 1
net.ipv4.conf.default.log_martians = 1
Run the following commands to set the active kernel parameters:
sysctl -w net.ipv4.conf.all.log_martians=1# sysctl -w net.ipv4.conf.default.log_martians=1# sysctl -w net.ipv4.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.2.5 Ensure broadcast ICMP requests are ignored

Severity

High

Description

Description Setting net.ipv4.icmp_echo_ignore_broadcasts to 1 will cause the system to ignore all ICMP echo and timestamp requests to broadcast and multicast addresses. Rationale Accepting ICMP echo and timestamp requests with broadcast or multicast destinations for your network could be used to trick your host into starting (or participating) in a Smurf attack. A Smurf attack relies on an attacker sending large amounts of ICMP broadcast messages with a spoofed source address. All hosts receiving this message and responding would send echo-reply messages back to the spoofed address, which is probably not routable. If many hosts respond to the packets, the amount of traffic on the network could be significantly multiplied.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.icmp_echo_ignore_broadcasts = 1
Run the following commands to set the active kernel parameters:
sysctl -w net.ipv4.icmp_echo_ignore_broadcasts=1# sysctl -w net.ipv4.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.2.6 Ensure bogus ICMP responses are ignored

Severity

High

Description

Description Setting icmp_ignore_bogus_error_responses to 1 prevents the kernel from logging bogus responses (RFC-1122 non-compliant) from broadcast reframes, keeping file systems from filling up with useless log messages. Rationale Some routers (and some attackers) will send responses that violate RFC-1122 and attempt to fill up a log file system with many useless error messages.

Recommendation

Set the following parameter in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.icmp_ignore_bogus_error_responses = 1 Run the following commands to set the active kernel parameters: # sysctl -w net.ipv4.icmp_ignore_bogus_error_responses=1# sysctl -w net.ipv4.route.flush=1

Failed Instances

i-079d0668bb45659b2

3.2.7 Ensure Reverse Path Filtering is enabled

Severity

High

Description

Description Setting net.ipv4.conf.all.rp_filter and net.ipv4.conf.default.rp_filter to 1 forces the Linux kernel to utilize reverse path filtering on a received packet to determine if the packet was valid. Essentially, with reverse path filtering, if the return packet does not go out the same interface that the corresponding source packet came from, the packet is dropped (and logged if log_martians is set). Rationale Setting these flags is a good way to deter attackers from sending your system bogus packets that cannot be responded to. One instance where this feature breaks down is if asymmetrical routing is employed. This would occur when using dynamic routing protocols (bgp, ospf, etc) on your system. If you are using asymmetrical routing on your system, you will not be able to enable this feature without breaking the routing.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file: net.ipv4.conf.all.rp_filter = 1net.ipv4.conf.default.rp_filter = 1 Run the following

```
commands to set the active kernel parameters: # sysctl -w net.ipv4.conf.all.rp_filter=1# sysctl -w net.ipv4.conf.default.rp_filter=1# sysctl -w net.ipv4.route.flush=1
```

Failed Instances

i-079d0668bb45659b2

3.2.8 Ensure TCP SYN Cookies is enabled

Severity

High

Description

Description When `tcp_syncookies` is set, the kernel will handle TCP SYN packets normally until the half-open connection queue is full, at which time, the SYN cookie functionality kicks in. SYN cookies work by not using the SYN queue at all. Instead, the kernel simply replies to the SYN with a SYN|ACK, but will include a specially crafted TCP sequence number that encodes the source and destination IP address and port number and the time the packet was sent. A legitimate connection would send the ACK packet of the three way handshake with the specially crafted sequence number. This allows the system to verify that it has received a valid response to a SYN cookie and allow the connection, even though there is no corresponding SYN in the queue. Rationale Attackers use SYN flood attacks to perform a denial of service attacked on a system by sending many SYN packets without completing the three way handshake. This will quickly use up slots in the kernel's half-open connection queue and prevent legitimate connections from succeeding. SYN cookies allow the system to keep accepting valid connections, even if under a denial of service attack.

Recommendation

Set the following parameters in `/etc/sysctl.conf` or a `/etc/sysctl.d/*` file:

`net.ipv4.tcp_syncookies = 1` Run the following commands to set the active kernel parameters: # `sysctl -w net.ipv4.tcp_syncookies=1# sysctl -w net.ipv4.route.flush=1`

Failed Instances

i-079d0668bb45659b2

3.2.9 Ensure IPv6 router advertisements are not accepted

Severity

High

Description

Description This setting disables the system's ability to accept IPv6 router advertisements. Rationale It is recommended that systems not accept router advertisements as they could be tricked into routing traffic to compromised machines. Setting hard routes within the system (usually a single default route to a trusted router) protects the system from bad routes.

Recommendation

Set the following parameters in /etc/sysctl.conf or a /etc/sysctl.d/* file:

```
net.ipv6.conf.all.accept_ra = 0net.ipv6.conf.default.accept_ra = 0 Run  
the following commands to set the active kernel parameters: # sysctl -w  
net.ipv6.conf.all.accept_ra=0# sysctl -w net.ipv6.conf.default.accept_ra=0# sysctl -w  
net.ipv6.route.flush=1
```

Failed Instances

i-079d0668bb45659b2

3.3.3 Ensure /etc/hosts.deny is configured

Severity

Informational

Description

Description The /etc/hosts.deny file specifies which IP addresses are not permitted to connect to the host. It is intended to be used in conjunction with the /etc/hosts.allow file.

Rationale The /etc/hosts.deny file serves as a failsafe so that any host not specified in /etc/hosts.allow is denied access to the system.

Recommendation

Run the following command to create /etc/hosts.deny : # echo "ALL: ALL" >> /etc/hosts.deny

Failed Instances

i-079d0668bb45659b2

3.4.1 Ensure DCCP is disabled

Severity

Informational

Description

Description The Datagram Congestion Control Protocol (DCCP) is a transport layer protocol that supports streaming media and telephony. DCCP provides a way to gain access to congestion control, without having to do it at the application layer, but does not provide in-sequence delivery. **Rationale** If the protocol is not required, it is recommended that the drivers not be installed to reduce the potential attack surface.

Recommendation

Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install dccp /bin/true

Failed Instances

i-079d0668bb45659b2

3.4.2 Ensure SCTP is disabled

Severity

Informational

Description

Description The Stream Control Transmission Protocol (SCTP) is a transport layer protocol used to support message oriented communication, with several streams of messages in one connection. It serves a similar function as TCP and UDP, incorporating features of both. It is message-oriented like UDP, and ensures reliable in-sequence transport of messages with congestion control like TCP. **Rationale** If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Recommendation

Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install sctp /bin/true

Failed Instances

i-079d0668bb45659b2

3.4.3 Ensure RDS is disabled

Severity

Informational

Description

Description The Reliable Datagram Sockets (RDS) protocol is a transport layer protocol designed to provide low-latency, high-bandwidth communications between cluster nodes. It was developed by the Oracle Corporation. **Rationale** If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Recommendation

Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install rds / bin/true

Failed Instances

i-079d0668bb45659b2

3.4.4 Ensure TIPC is disabled

Severity

Informational

Description

Description The Transparent Inter-Process Communication (TIPC) protocol is designed to provide communication between cluster nodes. **Rationale** If the protocol is not being used, it is recommended that kernel module not be loaded, disabling the service to reduce the potential attack surface.

Recommendation

Edit or create the file /etc/modprobe.d/CIS.conf and add the following line: install tipc / bin/true

Failed Instances

i-079d0668bb45659b2

3.5.1.1 Ensure default deny firewall policy

Severity

High

Description

Description A default deny all policy on connections ensures that any unconfigured network usage will be rejected. **Rationale** With a default accept policy the firewall will

accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Recommendation

Run the following commands to implement a default DROP policy: # iptables -P INPUT DROP# iptables -P OUTPUT DROP# iptables -P FORWARD DROP

Failed Instances

i-079d0668bb45659b2

3.5.1.2 Ensure loopback traffic is configured

Severity

High

Description

Description Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (127.0.0.0/8). Rationale Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (127.0.0.0/8) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Recommendation

Run the following commands to implement the loopback rules: # iptables -A INPUT -i lo -j ACCEPT# iptables -A OUTPUT -o lo -j ACCEPT# iptables -A INPUT -s 127.0.0.0/8 -j DROP

Failed Instances

i-079d0668bb45659b2

3.5.1.4 Ensure firewall rules exist for all open ports

Severity

High

Description

Description Any ports that have been opened on non-loopback addresses need firewall rules to govern traffic. Rationale Without a firewall rule configured for open ports default firewall policy will drop all packets to these ports.

Recommendation

For each port identified in the audit which does not have a firewall rule establish a proper rule for accepting inbound connections: # iptables -A INPUT -p <protocol> --dport <port> -m state --state NEW -j ACCEPT

Failed Instances

i-079d0668bb45659b2

3.5.2.1 Ensure IPv6 default deny firewall policy

Severity

High

Description

Description A default deny all policy on connections ensures that any unconfigured network usage will be rejected. Rationale With a default accept policy the firewall will accept any packet that is not configured to be denied. It is easier to white list acceptable usage than to black list unacceptable usage.

Recommendation

Run the following commands to implement a default DROP policy: # ip6tables -P INPUT DROP# ip6tables -P OUTPUT DROP# ip6tables -P FORWARD DROP

Failed Instances

i-079d0668bb45659b2

3.5.2.2 Ensure IPv6 loopback traffic is configured

Severity

High

Description

Description Configure the loopback interface to accept traffic. Configure all other interfaces to deny traffic to the loopback network (::1). Rationale Loopback traffic is generated between processes on machine and is typically critical to operation of the system. The loopback interface is the only place that loopback network (::1) traffic should be seen, all other interfaces should ignore traffic on this network as an anti-spoofing measure.

Recommendation

Run the following commands to implement the loopback rules:
ip6tables -A INPUT -i lo -j ACCEPT# ip6tables -A OUTPUT -o lo -j ACCEPT# ip6tables -A INPUT -s ::1 -j DROP

Failed Instances

i-079d0668bb45659b2

4.1.3 Ensure auditing for processes that start prior to auditd is enabled

Severity

High

Description

Description Configure grub so that processes that are capable of being audited can be audited even if they start up prior to auditd startup. Rationale Audit events need to be captured on processes that start up prior to auditd, so that potential malicious activity cannot go undetected.

Recommendation

Edit /etc/default/grub and add audit=1 to GRUB_CMDLINE_LINUX:
GRUB_CMDLINE_LINUX="audit=1" Run the following command to update the grub2 configuration: # grub2-mkconfig -o /boot/grub2/grub.cfg

Failed Instances

i-079d0668bb45659b2

4.1.4 Ensure events that modify date and time information are collected

Severity

High

Description

Description Capture events where the system date and/or time has been modified. The parameters in this section are set to determine if the adjtimex (tune kernel clock), settimofday (Set time, using timeval and timezone structures) stime (using seconds since 1/1/1970) or clock_settime (allows for the setting of several internal clocks and timers) system calls have been executed and always write an audit record to the /var/log/audit.log file upon exit, tagging the records with the identifier "time-change" Rationale Unexpected changes in system date and/or time could be a sign of malicious activity on the system.

Recommendation

For 32 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b32 -S adjtimex -S settimofday -S stime -k time-change-a
always,exit -F arch=b32 -S clock_settime -k time-change-w /etc/localtime -p wa -k time-change
For 64 bit systems add the following lines to the /etc/audit/audit.rules file:
-a always,exit -F arch=b64 -S adjtimex -S settimofday -k time-change-a always,exit
-F arch=b32 -S adjtimex -S settimofday -S stime -k time-change-a always,exit -F
arch=b64 -S clock_settime -k time-change-a always,exit -F arch=b32 -S clock_settime -k time-change-w /etc/localtime -p wa -k time-change

Failed Instances

i-079d0668bb45659b2

4.1.5 Ensure events that modify user/group information are collected

Severity

High

Description

Description Record events affecting the group , passwd (user IDs), shadow and gshadow (passwords) or /etc/security/opasswd (old passwords, based on remember parameter in the PAM configuration) files. The parameters in this section will watch the files to see if they have been opened for write or have had attribute changes (e.g. permissions) and tag them with the identifier "identity" in the audit log file. Rationale Unexpected changes to these files could be an indication that the system has been compromised and that an unauthorized user is attempting to hide their activities or compromise additional accounts.

Recommendation

Add the following lines to the /etc/audit/rules.d/audit.rules file: -w /etc/group -p wa -k identity-w /etc/passwd -p wa -k identity-w /etc/gshadow -p wa -k identity-w /etc/shadow -p wa -k identity-w /etc/security/opasswd -p wa -k identity

Failed Instances

i-079d0668bb45659b2

4.1.6 Ensure events that modify the system's network environment are collected

Severity

High

Description

Description Record changes to network environment files or system calls. The below parameters monitor the sethostname (set the systems host name) or setdomainname (set the systems domainname) system calls, and write an audit event on system call exit. The other parameters monitor the /etc/issue and /etc/issue.net files (messages displayed pre-login), /etc/hosts (file containing host names and associated IP addresses), /etc/sysconfig/network file and /etc/sysconfig/network-scripts/ directory (containing network interface scripts and configurations). Rationale Monitoring sethostname and setdomainname will identify potential unauthorized changes to host and domainname of a system. The changing of these names could potentially break security parameters that are set based on those names. The /etc/hosts file is monitored for changes in the file that can indicate an unauthorized intruder is trying to change machine associations with IP addresses and trick users and processes into connecting to unintended machines. Monitoring /etc/issue and /etc/issue.net is important, as intruders could put disinformation into those files and trick users into providing information to the intruder. Monitoring /etc/sysconfig/network and /etc/sysconfig/network-scripts/ is important as it can show if network interfaces or scripts are being modified in a way that can lead to the machine becoming unavailable or compromised. All audit records will be tagged with the identifier "system-locale."

Recommendation

For 32 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale-w /etc/issue -p wa -k system-locale-w /etc/issue.net -p wa -k system-locale-w /etc/hosts -p wa -k system-locale-w /etc/sysconfig/network -p wa -k system-locale-w /etc/sysconfig/network-scripts/ -p wa -k system-locale For 64 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b64 -S sethostname -S setdomainname -k system-locale -a always,exit -F arch=b32 -S sethostname -S setdomainname -k system-locale-w /etc/issue -p wa -k system-locale-w /etc/issue.net -p wa -k system-locale-w /etc/hosts -p wa -k system-locale-w /etc/sysconfig/network -p wa -k system-locale-w /etc/sysconfig/network-scripts/ -p wa -k system-locale

Failed Instances

i-079d0668bb45659b2

4.1.7 Ensure events that modify the system's Mandatory Access Controls are collected

Severity

High

Description

Description Monitor SELinux mandatory access controls. The parameters below monitor any write access (potential additional, deletion or modification of files in the directory) or attribute changes to the /etc/selinux or directory. Rationale Changes to files in these directories could indicate that an unauthorized user is attempting to modify access controls and change security contexts, leading to a compromise of the system.

Recommendation

Add the following lines to the /etc/audit/rules.d/audit.rules file: -w /etc/selinux/ -p wa -k MAC-policy-w /usr/share/selinux/ -p wa -k MAC-policy

Failed Instances

i-079d0668bb45659b2

4.1.8 Ensure login and logout events are collected

Severity

High

Description

Description Monitor login and logout events. The parameters below track changes to files associated with login/logout events. The file /var/log/lastlog maintain records of the last time a user successfully logged in. The /var/run/faillock directory maintains records of login failures via the pam_faillock module. Rationale Monitoring login/logout events could provide a system administrator with information associated with brute force attacks against user logins.

Recommendation

Add the following lines to the /etc/audit/rules.d/audit.rules file: -w /var/log/lastlog -p wa -k logins-w /var/run/faillock/ -p wa -k logins

Failed Instances

i-079d0668bb45659b2

4.1.9 Ensure session initiation information is collected

Severity

High

Description

Description Monitor session initiation events. The parameters in this section track changes to the files associated with session events. The file /var/run/utmp file tracks all currently logged in users. All audit records will be tagged with the identifier "session." The /var/log/wtmp file tracks logins, logouts, shutdown, and reboot events. The file /var/log/btmp keeps track of failed login attempts and can be read by entering the command /usr/bin/last -f /var/log/btmp . All audit records will be tagged with the identifier "logins." Rationale Monitoring these files for changes could alert a system administrator to logins occurring at unusual hours, which could indicate intruder activity (i.e. a user logging in at a time when they do not normally log in).

Recommendation

Add the following lines to the /etc/audit/rules.d/audit.rules file: -w /var/run/utmp -p wa -k session-w /var/log/wtmp -p wa -k logins-w /var/log/btmp -p wa -k logins

Failed Instances

i-079d0668bb45659b2

4.1.10 Ensure discretionary access control permission modification events are collected

Severity

High

Description

Description Monitor changes to file permissions, attributes, ownership and group. The parameters in this section track changes for system calls that affect file permissions and attributes. The chmod , fchmod and fchmodat system calls affect the permissions associated with a file. The chown , fchown , fchownat and lchown system calls affect owner and group attributes on a file. The setxattr , lsetxattr , fsetxattr (set extended file attributes) and removexattr , lremovexattr , fremovexattr (remove extended file attributes) control extended file attributes. In all cases, an audit record will only be written for non-system user ids (auid >= 1000) and will ignore Daemon events (auid = 4294967295). All audit records will be tagged with the identifier "perm_mod."

Rationale Monitoring for changes in file attributes could alert a system administrator to activity that could indicate intruder activity or policy violation.

Recommendation

For 32 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file:
-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod For 64 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod-a always,exit -F arch=b32 -S chmod -S fchmod -S fchmodat -F auid>=1000 -F auid!=4294967295 -k perm_mod-a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod-a always,exit -F arch=b32 -S chown -S fchown -S fchownat -S lchown -F auid>=1000 -F auid!=4294967295 -k perm_mod-a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod-a always,exit -F arch=b32 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -F auid>=1000 -F auid!=4294967295 -k perm_mod

Failed Instances

i-079d0668bb45659b2

4.1.11 Ensure unsuccessful unauthorized file access attempts are collected

Severity

High

Description

Description Monitor for unsuccessful attempts to access files. The parameters below are associated with system calls that control creation (creat), opening (open , openat) and truncation (truncate , ftruncate) of files. An audit log record will only be written if the user is a non-privileged user (auid >= 1000), is not a Daemon event (auid=4294967295) and if the system call returned EACCES (permission denied to the file) or EPERM (some other permanent error associated with the specific system call). All audit records will be tagged with the identifier "access." Rationale Failed attempts to open, create or truncate files could be an indication that an individual or process is trying to gain unauthorized access to the system.

Recommendation

For 32 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access For 64 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EACCES -F auid>=1000 -F auid!=4294967295 -k access-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access-a always,exit -F arch=b64 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access-a always,exit -F arch=b32 -S creat -S open -S openat -S truncate -S ftruncate -F exit=-EPERM -F auid>=1000 -F auid!=4294967295 -k access

Failed Instances

i-079d0668bb45659b2

4.1.13 Ensure successful file system mounts are collected

Severity

High

Description

Description Monitor the use of the mount system call. The mount (and umount) system call controls the mounting and unmounting of file systems. The parameters below configure the system to create an audit record when the mount system call is used by a non-privileged user Rationale It is highly unusual for a non privileged user to mount file systems to the system. While tracking mount commands gives the system administrator evidence that external media may have been mounted (based on a review of the source of the mount and confirming it's an external media type), it does not conclusively indicate that data was exported to the media. System administrators who wish to determine if data were exported, would also have to track successful open , creat and truncate system calls requiring write access to a file under the mount point of the external media file system. This could give a fair indication that a write occurred. The only way to truly prove it, would be to track successful writes to the external media. Tracking write system calls could quickly fill up the audit log and is not recommended. Recommendations on configuration options to track data export to media is beyond the scope of this document.

Recommendation

For 32 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -
a always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts
For 64 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a
always,exit -F arch=b64 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts-a
always,exit -F arch=b32 -S mount -F auid>=1000 -F auid!=4294967295 -k mounts

Failed Instances

i-079d0668bb45659b2

4.1.14 Ensure file deletion events by users are collected

Severity

High

Description

Description Monitor the use of system calls associated with the deletion or renaming of files and file attributes. This configuration statement sets up monitoring for the unlink (remove a file), unlinkat (remove a file attribute), rename (rename a file) and renameat (rename a file attribute) system calls and tags them with the identifier "delete". Rationale Monitoring these calls from non-privileged users could provide a system administrator with evidence that inappropriate removal of files and file attributes associated with protected files is occurring. While this audit option will look at all events, system administrators will want to look for specific privileged files that are being deleted or altered.

Recommendation

For 32 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -a
always,exit -F arch=b32 -S unlink -S unlinkat -S rename -S renameat -F auid>=1000
-F auid!=4294967295 -k delete For 64 bit systems add the following lines to the /etc/
audit/rules.d/audit.rules file: -a always,exit -F arch=b64 -S unlink -S unlinkat -S rename
-S renameat -F auid>=1000 -F auid!=4294967295 -k delete-a always,exit -F arch=b32
-S unlink -S unlinkat -S rename -S renameat -F auid>=1000 -F auid!=4294967295 -k
delete

Failed Instances

i-079d0668bb45659b2

4.1.15 Ensure changes to system administration scope (sudoers) is collected

Severity

High

Description

Description Monitor scope changes for system administrations. If the system has been properly configured to force system administrators to log in as themselves first and then use the sudo command to execute privileged commands, it is possible to monitor changes in scope. The file /etc/sudoers will be written to when the file or its attributes have changed. The audit records will be tagged with the identifier "scope." Rationale Changes in the /etc/sudoers file can indicate that an unauthorized change has been made to scope of system administrator activity.

Recommendation

Add the following line to the /etc/audit/rules.d/audit.rules file: -w /etc/sudoers -p wa -k scope-w /etc/sudoers.d/ -p wa -k scope

Failed Instances

i-079d0668bb45659b2

4.1.16 Ensure system administrator actions (sudolog) are collected

Severity

High

Description

Description Monitor the sudo log file. If the system has been properly configured to disable the use of the su command and force all administrators to have to log in first and then use sudo to execute privileged commands, then all administrator commands will be logged to /var/log/sudo.log . Any time a command is executed, an audit event will be triggered as the /var/log/sudo.log file will be opened for write and the executed administration command will be written to the log. Rationale Changes in /var/log/ sudo.log indicate that an administrator has executed a command or the log file itself has been tampered with. Administrators will want to correlate the events written to the audit trail with the records written to /var/log/sudo.log to verify if unauthorized commands have been executed.

Recommendation

Add the following lines to the /etc/audit/rules.d/audit.rules file: -w /var/log/sudo.log -p wa -k actions

Failed Instances

i-079d0668bb45659b2

4.1.17 Ensure kernel module loading and unloading is collected

Severity

High

Description

Description Monitor the loading and unloading of kernel modules. The programs insmod (install a kernel module), rmmod (remove a kernel module), and modprobe (a more sophisticated program to load and unload modules, as well as some other features) control loading and unloading of modules. The init_module (load a module) and delete_module (delete a module) system calls control loading and unloading of modules. Any execution of the loading and unloading module programs and system calls will trigger an audit record with an identifier of "modules". Rationale Monitoring the use of insmod , rmmod and modprobe could provide system administrators with evidence that an unauthorized user loaded or unloaded a kernel module, possibly compromising the security of the system. Monitoring of the init_module and delete_module system calls would reflect an unauthorized user attempting to use a different program to load and unload modules.

Recommendation

For 32 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -w /sbin/insmod -p x -k modules-w /sbin/rmmod -p x -k modules-w /sbin/modprobe -p x -k modules-a always,exit -F arch=b32 -S init_module -S delete_module -k modules

For 64 bit systems add the following lines to the /etc/audit/rules.d/audit.rules file: -w /sbin/insmod -p x -k modules-w /sbin/rmmod -p x -k modules-w /sbin/modprobe -p x -k modules-a always,exit -F arch=b64 -S init_module -S delete_module -k modules

Failed Instances

i-079d0668bb45659b2

4.1.18 Ensure the audit configuration is immutable

Severity

High

Description

Description Set system audit so that audit rules cannot be modified with auditctl . Setting the flag "-e 2" forces audit to be put in immutable mode. Audit changes can only be made on system reboot. Rationale In immutable mode, unauthorized users cannot execute changes to the audit system to potentially hide malicious activity and then put the audit rules back. Users would most likely notice a system reboot and that could alert administrators of an attempt to make unauthorized audit changes.

Recommendation

Add the following line to the end of the /etc/audit/rules.d/audit.rules file. -e 2

Failed Instances

i-079d0668bb45659b2

4.1.1.2 Ensure system is disabled when audit logs are full

Severity

High

Description

Description The auditd daemon can be configured to halt the system when the audit logs are full. Rationale In high security contexts, the risk of detecting unauthorized access or nonrepudiation exceeds the benefit of the system's availability.

Recommendation

Set the following parameters in /etc/audit/auditd.conf: space_left_action = emailaction_mail_acct = rootadmin_space_left_action = halt

Failed Instances

i-079d0668bb45659b2

4.1.1.3 Ensure audit logs are not automatically deleted

Severity

High

Description

Description The max_log_file_action setting determines how to handle the audit log file reaching the max file size. A value of keep_logs will rotate the logs but never delete old logs. Rationale In high security contexts, the benefits of maintaining a long audit history exceed the cost of storing the audit history.

Recommendation

Set the following parameter in /etc/audit/auditd.conf: max_log_file_action = keep_logs

Failed Instances

i-079d0668bb45659b2

4.2.4 Ensure permissions on all logfiles are configured

Severity

High

Description

Description Log files stored in /var/log/ contain logged information from many services on the system, or on log hosts others as well. Rationale It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Recommendation

Run the following command to set permissions on all existing log files: # find -L /var/log -type f -exec chmod g-wx,o-rwx {} +

Failed Instances

i-079d0668bb45659b2

4.2.1.3 Ensure rsyslog default file permissions configured

Severity

High

Description

Description rsyslog will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files. Rationale It is important to ensure that log files have the correct permissions to ensure that sensitive data is archived and protected.

Recommendation

Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and set \$FileCreateMode to 0640 or more restrictive: \$FileCreateMode 0640

Failed Instances

i-079d0668bb45659b2

4.2.1.4 Ensure rsyslog is configured to send logs to a remote log host

Severity

High

Description

Description The rsyslog utility supports the ability to send logs it gathers to a remote log host running syslogd(8) or to receive messages from remote hosts, reducing administrative overhead. Rationale Storing log data on a remote host protects log integrity from local attacks. If an attacker gains root access on the local system, they could tamper with or remove log data that is stored on the local system

Recommendation

Edit the /etc/rsyslog.conf and /etc/rsyslog.d/*.conf files and add the following line (where loghost.example.com is the name of your central log host). *.*

@@loghost.example.com Run the following command to reload the rsyslogd configuration: # pkill -HUP rsyslogd

Failed Instances

i-079d0668bb45659b2

5.6 Ensure access to the su command is restricted

Severity

High

Description

Description The su command allows a user to run a command or shell as another user. The program has been superseded by sudo , which allows for more granular control over privileged access. Normally, the su command can be executed by any user. By uncommenting the pam_wheel.so statement in /etc/pam.d/su , the su command will only allow users in the wheel group to execute su . Rationale Restricting the use of su , and using sudo in its place, provides system administrators better control of the escalation of user privileges to execute privileged commands. The sudo utility also provides a better logging and audit mechanism, as it can log each command executed via sudo , whereas su can only record that a user executed the su program.

Recommendation

Add the following line to the /etc/pam.d/su file: auth required pam_wheel.so use_uid
Create a comma separated list of users in the wheel statement in the /etc/group file:
wheel:x:10:root,<user list>

Failed Instances

i-079d0668bb45659b2

5.1.2 Ensure permissions on /etc/crontab are configured

Severity

High

Description

Description The /etc/crontab file is used by cron to control its own jobs. The commands in this item make sure that root is the user and group owner of the file and that only the owner can access the file. Rationale This file contains information on what system jobs are run by cron. Write access to these files could provide unprivileged users with the ability to elevate their privileges. Read access to these files could provide users with the ability to gain insight on system jobs that run on the system and could provide them a way to gain unauthorized privileged access.

Recommendation

Run the following commands to set ownership and permissions on /etc/crontab : #
chown root:root /etc/crontab# chmod og-rwx /etc/crontab

Failed Instances

i-079d0668bb45659b2

5.1.3 Ensure permissions on /etc/cron.hourly are configured

Severity

High

Description

Description This directory contains system cron jobs that need to run on an hourly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated

privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation

Run the following commands to set ownership and permissions on /etc/cron.hourly : # chown root:root /etc/cron.hourly# chmod og-rwx /etc/cron.hourly

Failed Instances

i-079d0668bb45659b2

5.1.4 Ensure permissions on /etc/cron.daily are configured

Severity

High

Description

Description The /etc/cron.daily directory contains system cron jobs that need to run on a daily basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation

Run the following commands to set ownership and permissions on /etc/cron.daily : # chown root:root /etc/cron.daily# chmod og-rwx /etc/cron.daily

Failed Instances

i-079d0668bb45659b2

5.1.5 Ensure permissions on /etc/cron.weekly are configured

Severity

High

Description

Description The /etc/cron.weekly directory contains system cron jobs that need to run on a weekly basis. The files in this directory cannot be manipulated by the

crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation

Run the following commands to set ownership and permissions on /etc/cron.weekly : # chown root:root /etc/cron.weekly# chmod og-rwx /etc/cron.weekly

Failed Instances

i-079d0668bb45659b2

5.1.6 Ensure permissions on /etc/cron.monthly are configured

Severity

High

Description

Description The /etc/cron.monthly directory contains system cron jobs that need to run on a monthly basis. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation

Run the following commands to set ownership and permissions on /etc/cron.monthly : # chown root:root /etc/cron.monthly# chmod og-rwx /etc/cron.monthly

Failed Instances

i-079d0668bb45659b2

5.1.7 Ensure permissions on /etc/cron.d are configured

Severity

High

Description

Description The /etc/cron.d directory contains system cron jobs that need to run in a similar manner to the hourly, daily weekly and monthly jobs from /etc/crontab , but require more granular control as to when they run. The files in this directory cannot be manipulated by the crontab command, but are instead edited by system administrators using a text editor. The commands below restrict read/write and search access to user and group root, preventing regular users from accessing this directory. Rationale Granting write access to this directory for non-privileged users could provide them the means for gaining unauthorized elevated privileges. Granting read access to this directory could give an unprivileged user insight in how to gain elevated privileges or circumvent auditing controls.

Recommendation

Run the following commands to set ownership and permissions on /etc/cron.d : # chown root:root /etc/cron.d# chmod og-rwx /etc/cron.d

Failed Instances

i-079d0668bb45659b2

5.1.8 Ensure at/cron is restricted to authorized users

Severity

High

Description

Description Configure /etc/cron.allow and /etc/at.allow to allow specific users to use these services. If /etc/cron.allow or /etc/at.allow do not exist, then /etc/at.deny and /etc/cron.deny are checked. Any user not specifically defined in those files is allowed to use at and cron. By removing the files, only users in /etc/cron.allow and /etc/at.allow are allowed to use at and cron. Note that even though a given user is not listed in cron.allow , cron jobs can still be run as that user. The cron.allow file only controls administrative access to the crontab command for scheduling and modifying cron jobs. Rationale On many systems, only the system administrator is authorized to schedule cron jobs. Using the cron.allow file to control who can run cron jobs enforces this policy. It is easier to manage an allow list than a deny list. In a deny list, you could potentially add a user ID to the system and forget to add it to the deny files.

Recommendation

Run the following commands to remove /etc/cron.deny and /etc/at.deny and create and set permissions and ownership for /etc/cron.allow and /etc/at.allow : # rm /etc/cron.deny# rm /etc/at.deny# touch /etc/cron.allow# touch /etc/at.allow# chmod og-rwx /etc/cron.allow# chmod og-rwx /etc/at.allow# chown root:root /etc/cron.allow# chown root:root /etc/at.allow

Failed Instances

i-079d0668bb45659b2

5.2.4 Ensure SSH Protocol is set to 2

Severity

High

Description

Description SSH supports two different and incompatible protocols: SSH1 and SSH2. SSH1 was the original protocol and was subject to security issues. SSH2 is more advanced and secure. Rationale SSH v1 suffers from insecurities that do not affect SSH v2.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows: Protocol 2

Failed Instances

i-079d0668bb45659b2

5.2.5 Ensure SSH LogLevel is appropriate

Severity

High

Description

Description INFO level is the basic level that only records login activity of SSH users. In many situations, such as Incident Response, it is important to determine when a particular user was active on a system. The logout record can eliminate those users who disconnected, which helps narrow the field. VERBOSE level specifies that login and logout activity as well as the key fingerprint for any SSH key used for login will be logged. This information is important for SSH key management, especially in legacy environments. Rationale SSH provides several logging levels with varying amounts of

verbosity. DEBUG is specifically not recommended other than strictly for debugging SSH communications since it provides so much data that it is difficult to identify important security information.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows: LogLevel VERBOSE or LogLevel INFO

Failed Instances

i-079d0668bb45659b2

5.2.6 Ensure SSH X11 forwarding is disabled

Severity

High

Description

Description The X11Forwarding parameter provides the ability to tunnel X11 traffic through the connection to enable remote graphic connections. Rationale Disable X11 forwarding unless there is an operational requirement to use X11 applications directly. There is a small risk that the remote X11 servers of users who are logged in via SSH with X11 forwarding could be compromised by other users on the X11 server. Note that even if X11 forwarding is disabled, users can always install their own forwarders.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows: X11Forwarding no

Failed Instances

i-079d0668bb45659b2

5.2.7 Ensure SSH MaxAuthTries is set to 4 or less

Severity

High

Description

Description The MaxAuthTries parameter specifies the maximum number of authentication attempts permitted per connection. When the login failure count reaches half the number, error messages will be written to the syslog file detailing the login failure. Rationale Setting the MaxAuthTries parameter to a low number will minimize

the risk of successful brute force attacks to the SSH server. While the recommended setting is 4, set the number based on site policy.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows: MaxAuthTries 4

Failed Instances

i-079d0668bb45659b2

5.2.8 Ensure SSH IgnoreRhosts is enabled

Severity

High

Description

Description The IgnoreRhosts parameter specifies that .rhosts and .shosts files will not be used in RhostsRSAAuthentication or HostbasedAuthentication . Rationale Setting this parameter forces users to enter a password when authenticating with ssh.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows: IgnoreRhosts yes

Failed Instances

i-079d0668bb45659b2

5.2.9 Ensure SSH HostbasedAuthentication is disabled

Severity

High

Description

Description The HostbasedAuthentication parameter specifies if authentication is allowed through trusted hosts via the user of .rhosts , or /etc/hosts.equiv , along with successful public key client host authentication. This option only applies to SSH Protocol Version 2. Rationale Even though the .rhosts files are ineffective if support is disabled in /etc/pam.conf , disabling the ability to use .rhosts files in SSH provides an additional layer of protection .

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows:
HostbasedAuthentication no

Failed Instances

i-079d0668bb45659b2

5.2.10 Ensure SSH root login is disabled

Severity

High

Description

Description The PermitRootLogin parameter specifies if the root user can log in using ssh(1). The default is no. Rationale Disallowing root logins over SSH requires system admins to authenticate using their own individual account, then escalating to root via sudo or su . This in turn limits opportunity for non-repudiation and provides a clear audit trail in the event of a security incident

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows: PermitRootLogin no

Failed Instances

i-079d0668bb45659b2

5.2.11 Ensure SSH PermitEmptyPasswords is disabled

Severity

High

Description

Description The PermitEmptyPasswords parameter specifies if the SSH server allows login to accounts with empty password strings. Rationale Disallowing remote shell access to accounts that have an empty password reduces the probability of unauthorized access to the system

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

PermitEmptyPasswords no

Failed Instances

i-079d0668bb45659b2

5.2.12 Ensure SSH PermitUserEnvironment is disabled

Severity

High

Description

Description The PermitUserEnvironment option allows users to present environment options to the ssh daemon. Rationale Permitting users the ability to set environment variables through the SSH daemon could potentially allow users to bypass security controls (e.g. setting an execution path that has ssh executing trojan'd programs)

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows:

PermitUserEnvironment no

Failed Instances

i-079d0668bb45659b2

5.2.13 Ensure only strong ciphers are used

Severity

High

Description

Description This variable limits the ciphers that SSH can use during communication. Rationale Weak ciphers that are used for authentication to the cryptographic module cannot be relied upon to provide confidentiality or integrity, and system data may be compromised. The DES, Triple DES, and Blowfish ciphers, as used in SSH, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, aka a "Sweet32" attack. The RC4 algorithm, as used in the TLS protocol and SSL protocol, does not properly combine state data with key data during the initialization phase, which makes it easier for remote attackers to conduct plaintext-recovery attacks against the initial bytes of a stream by sniffing network traffic that occasionally relies on keys affected by the Invariance Weakness, and then using a brute-force approach involving LSB values, aka the "Bar Mitzvah" issue. The passwords used during an SSH session encrypted with RC4 can be recovered by an attacker who is able to capture and replay the session Error handling in the SSH protocol; Client and Server, when using a block cipher algorithm in Cipher Block Chaining (CBC) mode, makes it easier for remote attackers to recover certain plaintext data from an arbitrary block of ciphertext in an SSH session via unknown vectors. The mm_newkeys_from_blob

function in monitor_wrap.c, when an AES-GCM cipher is used, does not properly initialize memory for a MAC context data structure, which allows remote authenticated users to bypass intended ForceCommand and login-shell restrictions via packet data that provides a crafted callback address

Recommendation

Edit the /etc/ssh/sshd_config file add/modify the Ciphers line to contain a comma separated list of the site approved ciphers Example: Ciphers chacha20-poly1305@openssh.com,aes256-gcm@openssh.com,aes128-gcm@openssh.com,aes256-ctr,aes192-ctr,aes128-ctr

Failed Instances

i-079d0668bb45659b2

5.2.14 Ensure only strong MAC algorithms are used

Severity

High

Description

Description This variable limits the types of MAC algorithms that SSH can use during communication. Rationale MD5 and 96-bit MAC algorithms are considered weak and have been shown to increase exploitability in SSH downgrade attacks. Weak algorithms continue to have a great deal of attention as a weak spot that can be exploited with expanded computing power. An attacker that breaks the algorithm could take advantage of a MiTM position to decrypt the SSH tunnel and capture credentials and information

Recommendation

Edit the /etc/ssh/sshd_config file and add/modify the MACs line to contain a comma separated list of the site approved MACs Example: MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,hmac-sha2-512,hmac-sha2-256

Failed Instances

i-079d0668bb45659b2

5.2.15 Ensure that strong Key Exchange algorithms are used

Severity

High

Description

Description Key exchange is any method in cryptography by which cryptographic keys are exchanged between two parties, allowing use of a cryptographic algorithm. If the sender and receiver wish to exchange encrypted messages, each must be equipped to encrypt messages to be sent and decrypt messages received Rationale Key exchange methods that are considered weak should be removed. A key exchange method may be weak because too few bits are used, or the hashing algorithm is considered too weak. Using weak algorithms could expose connections to man-in-the-middle attacks

Recommendation

Edit the /etc/ssh/sshd_config file add/modify the KexAlgorithms line to contain a comma separated list of the site approved key exchange algorithms Example: KexAlgorithms curve25519-sha256,curve25519-sha256@libssh.org,diffie-hellman-group14-sha256,diffie-hellman-group16-sha512,diffie-hellman-group18-sha512,ecdh-sha2-nistp521,ecdh-sha2-nistp384,ecdh-sha2-nistp256,diffie-hellman-group-exchange-sha256

Failed Instances

i-079d0668bb45659b2

5.2.16 Ensure SSH Idle Timeout Interval is configured

Severity

High

Description

Description The two options ClientAliveInterval and ClientAliveCountMax control the timeout of ssh sessions. When the ClientAliveInterval variable is set, ssh sessions that have no activity for the specified length of time are terminated. When the ClientAliveCountMax variable is set, sshd will send client alive messages at every ClientAliveInterval interval. When the number of consecutive client alive messages are sent with no response from the client, the ssh session is terminated. For example, if the ClientAliveInterval is set to 15 seconds and the ClientAliveCountMax is set to 3, the client ssh session will be terminated after 45 seconds of idle time. Rationale Having no timeout value associated with a connection could allow an unauthorized user access to another user's ssh session (e.g. user walks away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening.. While the recommended setting is 300 seconds (5 minutes), set this timeout value based on site policy. The recommended setting for ClientAliveCountMax is 0. In this case, the client

session will be terminated after 5 minutes of idle time and no keepalive messages will be sent.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameters according to site policy:
ClientAliveInterval 300 ClientAliveCountMax 0

Failed Instances

i-079d0668bb45659b2

5.2.17 Ensure SSH LoginGraceTime is set to one minute or less

Severity

High

Description

Description The LoginGraceTime parameter specifies the time allowed for successful authentication to the SSH server. The longer the Grace period is the more open unauthenticated connections can exist. Like other session controls in this session the Grace Period should be limited to appropriate organizational limits to ensure the service is available for needed access. Rationale Setting the LoginGraceTime parameter to a low number will minimize the risk of successful brute force attacks to the SSH server. It will also limit the number of concurrent unauthenticated connections While the recommended setting is 60 seconds (1 Minute), set the number based on site policy.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows: LoginGraceTime 60

Failed Instances

i-079d0668bb45659b2

5.2.18 Ensure SSH access is limited

Severity

High

Description

Description There are several options available to limit which users and group can access the system via SSH. It is recommended that at least one of the following options be leveraged: AllowUsers The AllowUsers variable gives the system administrator

the option of allowing specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by only allowing the allowed users to log in from a particular host, the entry can be specified in the form of user@host. AllowGroups The AllowGroups variable gives the system administrator the option of allowing specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable. DenyUsers The DenyUsers variable gives the system administrator the option of denying specific users to ssh into the system. The list consists of space separated user names. Numeric user IDs are not recognized with this variable. If a system administrator wants to restrict user access further by specifically denying a user's access from a particular host, the entry can be specified in the form of user@host. DenyGroups The DenyGroups variable gives the system administrator the option of denying specific groups of users to ssh into the system. The list consists of space separated group names. Numeric group IDs are not recognized with this variable. Rationale Restricting which users can remotely access the system via SSH will help ensure that only authorized users access the system.

Recommendation

Edit the /etc/ssh/sshd_config file to set one or more of the parameter as follows:
AllowUsers <userlist>AllowGroups <grouplist>DenyUsers <userlist>DenyGroups
<grouplist>

Failed Instances

i-079d0668bb45659b2

5.2.19 Ensure SSH warning banner is configured

Severity

High

Description

Description The Banner parameter specifies a file whose contents must be sent to the remote user before authentication is permitted. By default, no banner is displayed. Rationale Banners are used to warn connecting users of the particular site's policy regarding connection. Presenting a warning message prior to the normal user login may assist the prosecution of trespassers on the computer system.

Recommendation

Edit the /etc/ssh/sshd_config file to set the parameter as follows: Banner /etc/issue.net

Failed Instances

i-079d0668bb45659b2

5.3.1 Ensure password creation requirements are configured

Severity

High

Description

Description The pam_pwquality.so module checks the strength of passwords. It performs checks such as making sure a password is not a dictionary word, it is a certain length, contains a mix of characters (e.g. alphabet, numeric, other) and more. The following are definitions of the pam_pwquality .so options. try_first_pass - retrieve the password from a previous stacked PAM module. If not available, then prompt the user for a password.retry=3 - Allow 3 tries before sending back a failure. The following options are set in the /etc/security/pwquality.conf file: minlen = 14 - password must be 14 characters or more.dcredit = -1 - provide at least one digit.ucredit = -1 - provide at least one uppercase character.ocredit = -1 - provide at least one special character.lcredit = -1 - provide at least one lowercase character. The settings shown above are one possible policy. Alter these values to conform to your own organization's password policies.

Rationale Strong passwords protect systems from being hacked through brute force methods.

Recommendation

Edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files to include the appropriate options for pam_pwquality.so and to conform to site policy: password requisite pam_pwquality.so try_first_pass retry=3 Edit /etc/security/pwquality.conf to add or update the following settings to conform to site policy: minlen = 14dcredit = -1ucredit = -1ocredit = -1lcredit = -1

Failed Instances

i-079d0668bb45659b2

5.3.2 Ensure lockout for failed password attempts is configured

Severity

High

Description

Description Lock out users after n unsuccessful consecutive login attempts. The first sets of changes are made to the PAM configuration files. The second set of changes are applied to the program specific PAM configuration file. The second set of changes must be applied to each program that will lock out users. Check the documentation for each secondary program for instructions on how to configure them to work with PAM. Set the lockout number to the policy in effect at your site. Rationale Locking out user IDs after n unsuccessful consecutive login attempts mitigates brute force password attacks against your systems.

Recommendation

Edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files and add the following pam_faillock.so lines surrounding a pam_unix.so line modify the pam_unix.so is [success=1 default=bad] as listed in both: auth required pam_faillock.so preauth audit silent deny=5 unlock_time=900auth [success=1 default=bad] pam_unix.so auth [default=die] pam_faillock.so authfail audit deny=5 unlock_time=900auth sufficient pam_faillock.so authsucc audit deny=5 unlock_time=900

Failed Instances

i-079d0668bb45659b2

5.3.3 Ensure password reuse is limited

Severity

High

Description

Description The /etc/security/opasswd file stores the users' old passwords and can be checked to ensure that users are not recycling recent passwords. Rationale Forcing users not to reuse their past 5 passwords make it less likely that an attacker will be able to guess the password. Note that these change only apply to accounts configured on the local system.

Recommendation

Edit the /etc/pam.d/password-auth and /etc/pam.d/system-auth files to include the remember option and conform to site policy as shown: password sufficient pam_unix.so remember=5 or password required pam_pwhistory.so remember=5

Failed Instances

i-079d0668bb45659b2

5.4.4 Ensure default user umask is 027 or more restrictive

Severity

High

Description

Description The default umask determines the permissions of files created by users. The user creating the file has the discretion of making their files and directories readable by others via the chmod command. Users who wish to allow their files and directories to be readable by others by default may choose a different default umask by inserting the umask command into the standard shell configuration files (.profile , .bashrc , etc.) in their home directories. **Rationale** Setting a very secure default value for umask ensures that users make a conscious choice about their file permissions. A default umask setting of 077 causes files and directories created by users to not be readable by any other user on the system. A umask of 027 would make files and directories readable by users in the same Unix group, while a umask of 022 would make files readable by every user on the system.

Recommendation

Edit the /etc/bashrc, /etc/profile and /etc/profile.d/* .sh files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows: umask 027

Failed Instances

i-079d0668bb45659b2

5.4.5 Ensure default user shell timeout is 900 seconds or less

Severity

High

Description

Description The default TMOUT determines the shell timeout for users. The TMOUT value is measured in seconds. **Rationale** Having no timeout value associated with a shell could allow an unauthorized user access to another user's shell session (e.g. user walks

away from their computer and doesn't lock the screen). Setting a timeout value at least reduces the risk of this happening.

Recommendation

Edit the /etc/bashrc and /etc/profile files (and the appropriate files for any other shell supported on your system) and add or edit any umask parameters as follows:
TMOUT=600

Failed Instances

i-079d0668bb45659b2

5.4.1.1 Ensure password expiration is 365 days or less

Severity

High

Description

Description The PASS_MAX_DAYS parameter in /etc/login.defs allows an administrator to force passwords to expire once they reach a defined age. It is recommended that the PASS_MAX_DAYS parameter be set to less than or equal to 365 days. **Rationale** The window of opportunity for an attacker to leverage compromised credentials or successfully compromise credentials via an online brute force attack is limited by the age of the password. Therefore, reducing the maximum age of a password also reduces an attacker's window of opportunity.

Recommendation

Set the PASS_MAX_DAYS parameter to conform to site policy in /etc/login.defs :
PASS_MAX_DAYS 90 Modify user parameters for all users with a password set to match: # chage --maxdays 90 <user>

Failed Instances

i-079d0668bb45659b2

5.4.1.2 Ensure minimum days between password changes is 7 or more

Severity

High

Description

Description The PASS_MIN_DAYS parameter in /etc/login.defs allows an administrator to prevent users from changing their password until a minimum number of days have passed since the last time the user changed their password. It is recommended that PASS_MIN_DAYS parameter be set to 7 or more days. **Rationale** By restricting the frequency of password changes, an administrator can prevent users from repeatedly changing their password in an attempt to circumvent password reuse controls.

Recommendation

Set the PASS_MIN_DAYS parameter to 7 in /etc/login.defs : PASS_MIN_DAYS 7
Modify user parameters for all users with a password set to match: # chage --mindays 7 <user>

Failed Instances

i-079d0668bb45659b2

5.4.1.4 Ensure inactive password lock is 30 days or less

Severity

High

Description

Description User accounts that have been inactive for over a given period of time can be automatically disabled. It is recommended that accounts that are inactive for 30 days after password expiration be disabled. **Rationale** Inactive accounts pose a threat to system security since the users are not logging in to notice failed login attempts or other anomalies.

Recommendation

Run the following command to set the default password inactivity period to 30 days: # useradd -D -f 30 Modify user parameters for all users with a password set to match: # chage --inactive 30 <user>

Failed Instances

i-079d0668bb45659b2

4.2: Findings details - Common Vulnerabilities and Exposures-1.1

CVE-2022-23825

Severity

Medium

Description

Aliases in the branch predictor may cause some AMD processors to predict the wrong branch type potentially leading to information disclosure.

Recommendation

Use your Operating System's update feature to update package kernel-0:5.10.130-118.517.amzn2, kernel-tools-0:5.10.130-118.517.amzn2. For more information see <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-23825>

Failed Instances

i-079d0668bb45659b2

CVE-2022-26373

Severity

Medium

Description

Non-transparent sharing of return predictor targets between contexts in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.

Recommendation

Use your Operating System's update feature to update package kernel-0:5.10.130-118.517.amzn2, kernel-tools-0:5.10.130-118.517.amzn2. For more information see <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26373>

Failed Instances

i-079d0668bb45659b2

CVE-2022-29900

Severity

Medium

Description

Mis-trained branch predictions for return instructions may allow arbitrary speculative code execution under certain microarchitecture-dependent conditions.

Recommendation

Use your Operating System's update feature to update package kernel-0:5.10.130-118.517.amzn2, kernel-tools-0:5.10.130-118.517.amzn2. For more information see <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29900>

Failed Instances

i-079d0668bb45659b2

CVE-2022-29901

Severity

Low

Description

Intel microprocessor generations 6 to 8 are affected by a new Spectre variant that is able to bypass their retpoline mitigation in the kernel to leak arbitrary data. An attacker with unprivileged user access can hijack return instructions to achieve arbitrary speculative code execution under certain microarchitecture-dependent conditions.

Recommendation

Use your Operating System's update feature to update package kernel-0:5.10.130-118.517.amzn2, kernel-tools-0:5.10.130-118.517.amzn2. For more information see <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29901>

Failed Instances

i-079d0668bb45659b2

CVE-2022-34903

Severity

High

Description

GnuPG through 2.3.6, in unusual situations where an attacker possesses any secret-key information from a victim's keyring and other constraints (e.g., use of GPGME) are met, allows signature forgery via injection into the status line.

Recommendation

Use your Operating System's update feature to update package gnupg2-0:2.0.22-5.amzn2.0.4. For more information see <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-34903>

Failed Instances

i-079d0668bb45659b2

CVE-2022-36123

Severity

High

Description

The Linux kernel before 5.18.13 lacks a certain clear operation for the block starting symbol (.bss). This allows Xen PV guest OS users to cause a denial of service or gain privileges.

Recommendation

Use your Operating System's update feature to update package kernel-0:5.10.130-118.517.amzn2, kernel-tools-0:5.10.130-118.517.amzn2. For more information see <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36123>

Failed Instances

i-079d0668bb45659b2

CVE-2022-36879

Severity

Medium

Description

An issue was discovered in the Linux kernel through 5.18.14. xfrm_expand_policies in net/xfrm/xfrm_policy.c can cause a refcount to be dropped twice.

Recommendation

Use your Operating System's update feature to update package kernel-0:5.10.130-118.517.amzn2, kernel-tools-0:5.10.130-118.517.amzn2. For more information see <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36879>

Failed Instances

i-079d0668bb45659b2

CVE-2022-36946

Severity

High

Description

nfqnl_mangle in net/netfilter/nfnetlink_queue.c in the Linux kernel through 5.18.14 allows remote attackers to cause a denial of service (panic) because, in the case of an nf_queue verdict with a one-byte nfta_payload attribute, an skb_pull can encounter a negative skb->len.

Recommendation

Use your Operating System's update feature to update package kernel-0:5.10.130-11.8.517.amzn2, kernel-tools-0:5.10.130-118.517.amzn2. For more information see <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-36946>

Failed Instances

i-079d0668bb45659b2

4.3: Findings details - Network Reachability-1.1

TCP port 111 (NFS) is reachable from the internet with active listener on instance

Severity

Informational

Description

A recognized port is reachable from the internet with a service listening

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 111

Failed Instances

i-079d0668bb45659b2

TCP port 111 (RPC) is reachable from the internet with active listener on instance

Severity

Informational

Description

A recognized port is reachable from the internet with a service listening

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 111

Failed Instances

i-079d0668bb45659b2

TCP port 1110 (NFS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 1110

Failed Instances

i-079d0668bb45659b2

TCP port 135 (RPC) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 135

Failed Instances

i-079d0668bb45659b2

TCP port 137 (NetBIOS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 137

Failed Instances

i-079d0668bb45659b2

TCP port 139 (NetBIOS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 139

Failed Instances

i-079d0668bb45659b2

TCP port 1433 (SQLServer) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 1433

Failed Instances

i-079d0668bb45659b2

TCP port 1512 (WINS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 1512

Failed Instances

i-079d0668bb45659b2

TCP port 1521 (Oracle) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 1521

Failed Instances

i-079d0668bb45659b2

TCP port 1630 (Oracle) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 1630

Failed Instances

i-079d0668bb45659b2

TCP port 20 (FTP) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 20

Failed Instances

i-079d0668bb45659b2

TCP port 2049 (NFS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 2049

Failed Instances

i-079d0668bb45659b2

TCP port 21 (FTP) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 21

Failed Instances

i-079d0668bb45659b2

TCP port 22 (SSH) is reachable from the internet with active listener on instance

Severity

Informational

Description

A recognized port is reachable from the internet with a service listening

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 22

Failed Instances

i-079d0668bb45659b2

TCP port 23 (Telnet) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 23

Failed Instances

i-079d0668bb45659b2

TCP port 27017 (MongoDB) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 27017

Failed Instances

i-079d0668bb45659b2

TCP port 27018 (MongoDB) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 27018

Failed Instances

i-079d0668bb45659b2

TCP port 27019 (MongoDB) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 27019

Failed Instances

i-079d0668bb45659b2

TCP port 28017 (MongoDB) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 28017

Failed Instances

i-079d0668bb45659b2

TCP port 3268 (Global Catalog LDAP) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 3268

Failed Instances

i-079d0668bb45659b2

TCP port 3269 (Global Catalog LDAP over TLS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 3269

Failed Instances

i-079d0668bb45659b2

TCP port 3306 (MySQL) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 3306

Failed Instances

i-079d0668bb45659b2

TCP port 3389 (RDP) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 3389

Failed Instances

i-079d0668bb45659b2

TCP port 389 (LDAP) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 389

Failed Instances

i-079d0668bb45659b2

TCP port 4045 (NFS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 4045

Failed Instances

i-079d0668bb45659b2

TCP port 42 (WINS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 42

Failed Instances

i-079d0668bb45659b2

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

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 443

Failed Instances

i-079d0668bb45659b2

TCP port 445 (SMB) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 445

Failed Instances

i-079d0668bb45659b2

TCP port 464 (Kerberos) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 464

Failed Instances

i-079d0668bb45659b2

TCP port 515 (Print Services) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 515

Failed Instances

i-079d0668bb45659b2

TCP port 530 (RPC) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 530

Failed Instances

i-079d0668bb45659b2

TCP port 543 (Kerberos) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 543

Failed Instances

i-079d0668bb45659b2

TCP port 5432 (PostgreSQL) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 5432

Failed Instances

i-079d0668bb45659b2

TCP port 544 (Kerberos) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 544

Failed Instances

i-079d0668bb45659b2

TCP port 546 (DHCP) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 546

Failed Instances

i-079d0668bb45659b2

TCP port 547 (DHCP) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 547

Failed Instances

i-079d0668bb45659b2

TCP port 601 (Syslog) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 601

Failed Instances

i-079d0668bb45659b2

TCP port 636 (LDAP over TLS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 636

Failed Instances

i-079d0668bb45659b2

TCP port 67 (DHCP) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 67

Failed Instances

i-079d0668bb45659b2

TCP port 711 is reachable from the internet with active listener on instance

Severity

Low

Description

An unrecognized port is reachable from the internet with a service listening

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 711

Failed Instances

i-079d0668bb45659b2

TCP port 749 (Kerberos) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 749

Failed Instances

i-079d0668bb45659b2

TCP port 751 (Kerberos) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 751

Failed Instances

i-079d0668bb45659b2

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

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 80

Failed Instances

i-079d0668bb45659b2

TCP port 88 (Kerberos) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 88

Failed Instances

i-079d0668bb45659b2

TCP port 9200 (Elasticsearch) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 9200

Failed Instances

i-079d0668bb45659b2

TCP port 9300 (Elasticsearch) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 9300

Failed Instances

i-079d0668bb45659b2

UDP port 111 (NFS) is reachable from the internet with active listener on instance

Severity

Informational

Description

A recognized port is reachable from the internet with a service listening

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 111

Failed Instances

i-079d0668bb45659b2

UDP port 111 (RPC) is reachable from the internet with active listener on instance

Severity

Informational

Description

A recognized port is reachable from the internet with a service listening

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 111

Failed Instances

i-079d0668bb45659b2

UDP port 1110 (NFS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 1110

Failed Instances

i-079d0668bb45659b2

UDP port 135 (RPC) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 135

Failed Instances

i-079d0668bb45659b2

UDP port 137 (NetBIOS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 137

Failed Instances

i-079d0668bb45659b2

UDP port 138 (NetBIOS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 138

Failed Instances

i-079d0668bb45659b2

UDP port 1434 (SQLServer) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 1434

Failed Instances

i-079d0668bb45659b2

UDP port 1512 (WINS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 1512

Failed Instances

i-079d0668bb45659b2

UDP port 20 (FTP) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 20

Failed Instances

i-079d0668bb45659b2

UDP port 2049 (NFS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 2049

Failed Instances

i-079d0668bb45659b2

UDP port 21 (FTP) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 21

Failed Instances

i-079d0668bb45659b2

UDP port 23 (Telnet) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 23

Failed Instances

i-079d0668bb45659b2

UDP port 3389 (RDP) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 3389

Failed Instances

i-079d0668bb45659b2

UDP port 4045 (NFS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 4045

Failed Instances

i-079d0668bb45659b2

UDP port 42 (WINS) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 42

Failed Instances

i-079d0668bb45659b2

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

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 443

Failed Instances

i-079d0668bb45659b2

UDP port 445 (SMB) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 445

Failed Instances

i-079d0668bb45659b2

UDP port 464 (Kerberos) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 464

Failed Instances

i-079d0668bb45659b2

UDP port 514 (Syslog) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 514

Failed Instances

i-079d0668bb45659b2

UDP port 515 (Print Services) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 515

Failed Instances

i-079d0668bb45659b2

UDP port 530 (RPC) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 530

Failed Instances

i-079d0668bb45659b2

UDP port 546 (DHCP) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 546

Failed Instances

i-079d0668bb45659b2

UDP port 547 (DHCP) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 547

Failed Instances

i-079d0668bb45659b2

UDP port 67 (DHCP) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 67

Failed Instances

i-079d0668bb45659b2

UDP port 68 (DHCP) is reachable from the internet with active listener on instance

Severity

Informational

Description

A recognized port is reachable from the internet with a service listening

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 68

Failed Instances

i-079d0668bb45659b2

UDP port 711 is reachable from the internet with active listener on instance

Severity

Low

Description

An unrecognized port is reachable from the internet with a service listening

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 711

Failed Instances

i-079d0668bb45659b2

UDP port 749 (Kerberos) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 749

Failed Instances

i-079d0668bb45659b2

UDP port 750 (Kerberos) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 750

Failed Instances

i-079d0668bb45659b2

UDP port 751 (Kerberos) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 751

Failed Instances

i-079d0668bb45659b2

UDP port 752 (Kerberos) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 752

Failed Instances

i-079d0668bb45659b2

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

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 80

Failed Instances

i-079d0668bb45659b2

UDP port 88 (Kerberos) is reachable from the internet with no listener on instance

Severity

Informational

Description

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

Recommendation

You can edit the Security Group sg-06dc22f88ded293b4 to remove access from the internet on port 88

Failed Instances

i-079d0668bb45659b2

4.4: 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-079d0668bb45659b2

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 - CIS Operating System Security Configuration Benchmarks-1.0

5.1.1 Level 1

Rule	Description
1.1.3 Ensure nodev option set on /tmp partition	<p>Description</p> <p>The nodev mount option specifies that the filesystem cannot contain special devices.</p> <p>Rationale</p> <p>Since the /tmp filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices in /tmp .</p>
1.1.4 Ensure nosuid option set on /tmp partition	<p>Description</p> <p>The nosuid mount option specifies that the filesystem cannot contain setuid files.</p> <p>Rationale</p> <p>Since the /tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot create setuid files in /tmp .</p>

<p>1.1.5 Ensure noexec option set on /tmp partition</p>	<p>Description</p> <p>The noexec mount option specifies that the filesystem cannot contain executable binaries.</p> <p>Rationale</p> <p>Since the /tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from /tmp .</p>
<p>1.1.8 Ensure nodev option set on /var/tmp partition</p>	<p>Description</p> <p>The nodev mount option specifies that the filesystem cannot contain special devices.</p> <p>Rationale</p> <p>Since the /var/tmp filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices in /var/tmp .</p>
<p>1.1.9 Ensure nosuid option set on /var/tmp partition</p>	<p>Description</p> <p>The nosuid mount option specifies that the filesystem cannot contain setuid files.</p> <p>Rationale</p> <p>Since the /var/tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot create setuid files in /var/tmp .</p>

1.1.10 Ensure noexec option set on /var/tmp partition	<p>Description</p> <p>The noexec mount option specifies that the filesystem cannot contain executable binaries.</p> <p>Rationale</p> <p>Since the /var/tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from /var/tmp .</p>
1.1.14 Ensure nodev option set on /home partition	<p>Description</p> <p>The nodev mount option specifies that the filesystem cannot contain special devices.</p> <p>Rationale</p> <p>Since the user partitions are not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices.</p>
1.1.15 Ensure nodev option set on /dev/shm partition	<p>Description</p> <p>The nodev mount option specifies that the filesystem cannot contain special devices.</p> <p>Rationale</p> <p>Since the /dev/shm filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create special devices in /dev/shm partitions.</p>

<p>1.1.16 Ensure nosuid option set on /dev/shm partition</p>	<p>Description</p> <p>The nosuid mount option specifies that the filesystem cannot contain setuid files.</p> <p>Rationale</p> <p>Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.</p>
<p>1.2.3 Ensure gpgcheck is globally activated</p>	<p>Description</p> <p>The gpgcheck option, found in the main section of the /etc/yum.conf and individual /etc/yum/repos.d/* files determines if an RPM package's signature is checked prior to its installation.</p> <p>Rationale</p> <p>It is important to ensure that an RPM's package signature is always checked prior to installation to ensure that the software is obtained from a trusted source.</p>
<p>1.4.1 Ensure permissions on bootloader config are configured</p>	<p>Description</p> <p>The grub configuration file contains information on boot settings and passwords for unlocking boot options. The grub configuration is usually located at /boot/grub2/grub.cfg and linked as /etc/grub2.cfg. Additional settings can be found in the /boot/grub2/user.cfg file.</p> <p>Rationale</p>

	<p>Setting the permissions to read and write for root only prevents non-root users from seeing the boot parameters or changing them. Non-root users who read the boot parameters may be able to identify weaknesses in security upon boot and be able to exploit them.</p>
1.4.2 Ensure authentication required for single user mode	<p>Description</p> <p>Single user mode (rescue mode) is used for recovery when the system detects an issue during boot or by manual selection from the bootloader.</p> <p>Rationale</p> <p>Requiring authentication in single user mode (rescue mode) prevents an unauthorized user from rebooting the system into single user to gain root privileges without credentials.</p>
1.5.3 Ensure prelink is disabled	<p>Description</p> <p>prelink is a program that modifies ELF shared libraries and ELF dynamically linked binaries in such a way that the time needed for the dynamic linker to perform relocations at startup significantly decreases.</p> <p>Rationale</p> <p>The prelinking feature can interfere with the operation of AIDE, because it changes binaries. Prelinking can also increase the vulnerability of the system if a malicious user is able to compromise a common library such as libc.</p>
1.7.1.4 Ensure permissions on /etc/motd are configured	<p>Description</p>

	<p>The contents of the /etc/motd file are displayed to users after login and function as a message of the day for authenticated users.</p> <p>Rationale</p> <p>If the /etc/motd file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.</p>
1.7.1.5 Ensure permissions on /etc/issue are configured	<p>Description</p> <p>The contents of the /etc/issue file are displayed to users prior to login for local terminals.</p> <p>Rationale</p> <p>If the /etc/issue file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.</p>
1.7.1.6 Ensure permissions on /etc/issue.net are configured	<p>Description</p> <p>The contents of the /etc/issue.net file are displayed to users prior to login for remote connections from configured services.</p> <p>Rationale</p> <p>If the /etc/issue.net file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.</p>
2.1.2 Ensure X Window System is not installed	Description

	<p>The X Window System provides a Graphical User Interface (GUI) where users can have multiple windows in which to run programs and various add on. The X Windows system is typically used on workstations where users login, but not on servers where users typically do not login.</p> <p>Rationale</p> <p>Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface.</p>
2.1.15 Ensure mail transfer agent is configured for local-only mode	<p>Description</p> <p>Mail Transfer Agents (MTA), such as sendmail and Postfix, are used to listen for incoming mail and transfer the messages to the appropriate user or mail server. If the system is not intended to be a mail server, it is recommended that the MTA be configured to only process local mail.</p> <p>Rationale</p> <p>The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.</p>
2.1.1.1 Ensure time synchronization is in use	<p>Description</p> <p>System time should be synchronized between all systems in an environment. This is typically done by establishing an authoritative time server or set of</p>

	<p>servers and having all systems synchronize their clocks to them.</p> <p>Rationale</p> <p>Time synchronization is important to support time sensitive security mechanisms like Kerberos and also ensures log files have consistent time records across the enterprise, which aids in forensic investigations.</p>
2.1.1.2 Ensure ntp is configured	<p>Description</p> <p>ntp is a daemon which implements the Network Time Protocol (NTP). It is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on NTP can be found at http://www.ntp.org. ntp can be configured to be a client and/or a server.</p> <p>This recommendation only applies if ntp is in use on the system.</p> <p>Rationale</p> <p>If ntp is in use on the system proper configuration is vital to ensuring time synchronization is working properly.</p>
2.1.1.3 Ensure chrony is configured	<p>Description</p> <p>chrony is a daemon which implements the Network Time Protocol (NTP) is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on chrony can be found at http://chrony.tuxfamily.org/. chrony can be configured to be a client and/or a server.</p>

	<p>Rationale</p> <p>If chrony is in use on the system proper configuration is vital to ensuring time synchronization is working properly.</p> <p>This recommendation only applies if chrony is in use on the system.</p>
2.2.1 Ensure NIS Client is not installed	<p>Description</p> <p>The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client (<code>ypbind</code>) was used to bind a machine to an NIS server and receive the distributed configuration files.</p> <p>Rationale</p> <p>The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.</p>
2.2.2 Ensure rsh client is not installed	<p>Description</p> <p>The <code>rsh</code> package contains the client commands for the <code>rsh</code> services.</p> <p>Rationale</p> <p>These legacy clients contain numerous security exposures and have been replaced with the more</p>

	<p>secure SSH package. Even if the server is removed, it is best to ensure the clients are also removed to prevent users from inadvertently attempting to use these commands and therefore exposing their credentials. Note that removing the rsh package removes the clients for rsh , rcp and rlogin .</p>
2.2.3 Ensure talk client is not installed	<p>Description</p> <p>The talk software makes it possible for users to send and receive messages across systems through a terminal session. The talk client, which allows initialization of talk sessions, is installed by default.</p> <p>Rationale</p> <p>The software presents a security risk as it uses unencrypted protocols for communication.</p>
2.2.4 Ensure telnet client is not installed	<p>Description</p> <p>The telnet package contains the telnet client, which allows users to start connections to other systems via the telnet protocol.</p> <p>Rationale</p> <p>The telnet protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The ssh package provides an encrypted session and stronger security and is included in most Linux distributions.</p>
2.2.5 Ensure LDAP client is not installed	<p>Description</p> <p>The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service</p>

	<p>that provides a method for looking up information from a central database.</p> <p>Rationale</p> <p>If the system will not need to act as an LDAP client, it is recommended that the software be removed to reduce the potential attack surface.</p>
3.3.1 Ensure TCP Wrappers is installed	<p>Description</p> <p>TCP Wrappers provides a simple access list and standardized logging method for services capable of supporting it. In the past, services that were called from inetd and xinetd supported the use of tcp wrappers. As inetd and xinetd have been falling in disuse, any service that can support tcp wrappers will have the libwrap.so library attached to it.</p> <p>Rationale</p> <p>TCP Wrappers provide a good simple access list mechanism to services that may not have that support built in. It is recommended that all services that can support TCP Wrappers, use it.</p>
3.3.2 Ensure /etc/hosts.allow is configured	<p>Description</p> <p>The /etc/hosts.allow file specifies which IP addresses are permitted to connect to the host. It is intended to be used in conjunction with the /etc/hosts.deny file.</p> <p>Rationale</p> <p>The /etc/hosts.allow file supports access control by IP and helps ensure that only authorized systems can connect to the system.</p>

3.3.4 Ensure permissions on /etc/hosts.allow are configured	<p>Description</p> <p>The /etc/hosts.allow file contains networking information that is used by many applications and therefore must be readable for these applications to operate.</p> <p>Rationale</p> <p>It is critical to ensure that the /etc/hosts.allow file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.</p>
3.3.5 Ensure permissions on /etc/hosts.deny are configured	<p>Description</p> <p>The /etc/hosts.deny file contains network information that is used by many system applications and therefore must be readable for these applications to operate.</p> <p>Rationale</p> <p>It is critical to ensure that the /etc/hosts.deny file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.</p>
3.5.3 Ensure iptables is installed	<p>Description</p> <p>iptables allows configuration of the IPv4 tables in the linux kernel and the rules stored within them. Most firewall configuration utilities operate as a front end to iptables.</p>

	<p>Rationale</p> <p>iptables is required for firewall management and configuration.</p>
4.2.3 Ensure rsyslog or syslog-ng is installed	<p>Description</p> <p>The rsyslog and syslog-ng software are recommended replacements to the original syslogd daemon which provide improvements over syslogd , such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server.</p> <p>Rationale</p> <p>The security enhancements of rsyslog and syslog-ng such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.</p>
4.2.2.1 Ensure syslog-ng service is enabled	<p>Description</p> <p>Once the syslog-ng package is installed it needs to be activated.</p> <p>Rationale</p> <p>If the syslog-ng service is not activated the system may default to the syslogd service or lack logging instead.</p>
4.2.2.3 Ensure syslog-ng default file permissions configured	<p>Description</p>

	<p>syslog-ng will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.</p> <p>Rationale</p> <p>It is important to ensure that log files exist and have the correct permissions to ensure that sensitive syslog-ng data is archived and protected.</p>
5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured	<p>Description</p> <p>The /etc/ssh/sshd_config file contains configuration specifications for sshd. The command below sets the owner and group of the file to root.</p> <p>Rationale</p> <p>The /etc/ssh/sshd_config file needs to be protected from unauthorized changes by non-privileged users.</p>
5.2.3 Ensure permissions on SSH public host key files are configured	<p>Description</p> <p>An SSH public key is one of two files used in SSH public key authentication. In this authentication method, a public key is a key that can be used for verifying digital signatures generated using a corresponding private key. Only a public key that corresponds to a private key will be able to authenticate successfully.</p> <p>Rationale</p> <p>If a public host key file is modified by an unauthorized user, the SSH service may be compromised.</p>

<p>5.3.4 Ensure password hashing algorithm is SHA-512</p>	<p>Description</p> <p>The commands below change password encryption from md5 to sha512 (a much stronger hashing algorithm). All existing accounts will need to perform a password change to upgrade the stored hashes to the new algorithm.</p> <p>Rationale</p> <p>The SHA-512 algorithm provides much stronger hashing than MD5, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.</p> <p>Note that these changes only apply to accounts configured on the local system.</p>
<p>5.4.2 Ensure system accounts are non-login</p>	<p>Description</p> <p>There are a number of accounts provided with Amazon Linux 2 that are used to manage applications and are not intended to provide an interactive shell.</p> <p>Rationale</p> <p>It is important to make sure that accounts that are not being used by regular users are prevented from being used to provide an interactive shell. By default Amazon Linux 2 sets the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to /sbin/nologin . This prevents the account from potentially being used to run any commands. Some built-in accounts use /bin/false which is also acceptable. This prevents the account from potentially being used to run any commands.</p>
<p>5.4.3 Ensure default group for the root account is GID 0</p>	<p>Description</p>

	<p>The usermod command can be used to specify which group the root user belongs to. This affects permissions of files that are created by the root user.</p> <p>Rationale</p> <p>Using GID 0 for the root account helps prevent root - owned files from accidentally becoming accessible to non-privileged users.</p>
6.1.2 Ensure permissions on /etc/passwd are configured	<p>Description</p> <p>The /etc/passwd file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.</p> <p>Rationale</p> <p>It is critical to ensure that the /etc/passwd file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.</p>
6.1.3 Ensure permissions on /etc/shadow are configured	<p>Description</p> <p>The /etc/shadow file is used to store the information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.</p> <p>Rationale</p> <p>If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed password to break it. Other security</p>

	<p>information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert the user accounts.</p>
6.1.4 Ensure permissions on /etc/group are configured	<p>Description</p> <p>The /etc/group file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.</p> <p>Rationale</p> <p>The /etc/group file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.</p>
6.1.5 Ensure permissions on /etc/gshadow are configured	<p>Description</p> <p>The /etc/gshadow file is used to store the information about groups that is critical to the security of those accounts, such as the hashed password and other security information.</p> <p>Rationale</p> <p>If attackers can gain read access to the /etc/gshadow file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the /etc/gshadow file (such as group administrators) could also be useful to subvert the group.</p>
6.1.6 Ensure permissions on /etc/passwd- are configured	<p>Description</p>

	<p>The /etc/passwd- file contains backup user account information.</p> <p>Rationale</p> <p>It is critical to ensure that the /etc/passwd- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.</p>
6.1.7 Ensure permissions on /etc/shadow- are configured	<p>Description</p> <p>The /etc/shadow- file is used to store backup information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.</p> <p>Rationale</p> <p>It is critical to ensure that the /etc/shadow- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.</p>
6.1.8 Ensure permissions on /etc/group- are configured	<p>Description</p> <p>The /etc/group- file contains a backup list of all the valid groups defined in the system.</p> <p>Rationale</p> <p>It is critical to ensure that the /etc/group- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.</p>

6.1.9 Ensure permissions on /etc/gshadow- are configured	<p>Description</p> <p>The /etc/gshadow- file is used to store backup information about groups that is critical to the security of those accounts, such as the hashed password and other security information.</p> <p>Rationale</p> <p>It is critical to ensure that the /etc/gshadow- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.</p>
6.2.2 Ensure no legacy "+" entries exist in /etc/passwd	<p>Description</p> <p>The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.</p> <p>Rationale</p> <p>These entries may provide an avenue for attackers to gain privileged access on the system.</p>
6.2.3 Ensure no legacy "+" entries exist in /etc/shadow	<p>Description</p> <p>The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.</p>

	<p>Rationale</p> <p>These entries may provide an avenue for attackers to gain privileged access on the system.</p>
6.2.4 Ensure no legacy "+" entries exist in /etc/group	<p>Description</p> <p>The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.</p> <p>Rationale</p> <p>These entries may provide an avenue for attackers to gain privileged access on the system.</p>
6.2.5 Ensure root is the only UID 0 account	<p>Description</p> <p>Any account with UID 0 has superuser privileges on the system.</p> <p>Rationale</p> <p>This access must be limited to only the default root account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in Item 5.6 Ensure access to the su command is restricted.</p>
6.2.6 Ensure root PATH Integrity	Description

	<p>The root user can execute any command on the system and could be fooled into executing programs unintentionally if the PATH is not set correctly.</p> <p>Rationale</p> <p>Including the current working directory (.) or other writable directory in root's executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as root to execute a Trojan horse program.</p>
6.2.7 Ensure all users' home directories exist	<p>Description</p> <p>Users can be defined in /etc/passwd without a home directory or with a home directory that does not actually exist.</p> <p>Rationale</p> <p>If the user's home directory does not exist or is unassigned, the user will be placed in "/" and will not be able to write any files or have local environment variables set.</p>
6.2.8 Ensure users' home directories permissions are 750 or more restrictive	<p>Description</p> <p>While the system administrator can establish secure permissions for users' home directories, the users can easily override these.</p> <p>Rationale</p> <p>Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.</p>

<p>6.2.9 Ensure users own their home directories</p>	<p>Description</p> <p>The user home directory is space defined for the particular user to set local environment variables and to store personal files.</p> <p>Rationale</p> <p>Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.</p>
<p>6.2.10 Ensure users' dot files are not group or world writable</p>	<p>Description</p> <p>While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.</p> <p>Rationale</p> <p>Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.</p>
<p>6.2.11 Ensure no users have .forward files</p>	<p>Description</p> <p>The .forward file specifies an email address to forward the user's mail to.</p> <p>Rationale</p> <p>Use of the .forward file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The .forward file also poses a risk as</p>

	<p>it can be used to execute commands that may perform unintended actions.</p>
6.2.12 Ensure no users have .netrc files	<p>Description</p> <p>The .netrc file contains data for logging into a remote host for file transfers via FTP.</p> <p>Rationale</p> <p>The .netrc file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over .netrc files from other systems which could pose a risk to those systems.</p>
6.2.13 Ensure users' .netrc Files are not group or world accessible	<p>Description</p> <p>While the system administrator can establish secure permissions for users' .netrc files, the users can easily override these.</p> <p>Rationale</p> <p>.netrc files may contain unencrypted passwords that may be used to attack other systems.</p>
6.2.14 Ensure no users have .rhosts files	<p>Description</p> <p>While no .rhosts files are shipped by default, users can easily create them.</p> <p>Rationale</p>

	<p>This action is only meaningful if .rhosts support is permitted in the file /etc/pam.conf . Even though the .rhosts files are ineffective if support is disabled in /etc/pam.conf , they may have been brought over from other systems and could contain information useful to an attacker for those other systems.</p>
6.2.15 Ensure all groups in /etc/passwd exist in /etc/group	<p>Description</p> <p>Over time, system administration errors and changes can lead to groups being defined in /etc/passwd but not in /etc/group .</p> <p>Rationale</p> <p>Groups defined in the /etc/passwd file but not in the /etc/group file pose a threat to system security since group permissions are not properly managed.</p>
6.2.16 Ensure no duplicate UIDs exist	<p>Description</p> <p>Although the useradd program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the /etc/passwd file and change the UID field.</p> <p>Rationale</p> <p>Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.</p>
6.2.17 Ensure no duplicate GIDs exist	<p>Description</p> <p>Although the groupadd program will not let you create a duplicate Group ID (GID), it is possible for an</p>

	<p>administrator to manually edit the /etc/group file and change the GID field.</p> <p>Rationale</p> <p>User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.</p>
6.2.18 Ensure no duplicate user names exist	<p>Description</p> <p>Although the useradd program will not let you create a duplicate user name, it is possible for an administrator to manually edit the /etc/passwd file and change the user name.</p> <p>Rationale</p> <p>If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in /etc/passwd . For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a security problem.</p>
6.2.19 Ensure no duplicate group names exist	<p>Description</p> <p>Although the groupadd program will not let you create a duplicate group name, it is possible for an administrator to manually edit the /etc/group file and change the group name.</p> <p>Rationale</p> <p>If a group is assigned a duplicate group name, it will create and have access to files with the first GID for</p>

	that group in /etc/group . Effectively, the GID is shared, which is a security problem.
--	---

5.1.2 Level 2

Rule	Description
1.1.3 Ensure nodev option set on /tmp partition	<p>Description</p> <p>The nodev mount option specifies that the filesystem cannot contain special devices.</p> <p>Rationale</p> <p>Since the /tmp filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices in /tmp .</p>
1.1.4 Ensure nosuid option set on /tmp partition	<p>Description</p> <p>The nosuid mount option specifies that the filesystem cannot contain setuid files.</p> <p>Rationale</p> <p>Since the /tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot create setuid files in /tmp .</p>
1.1.5 Ensure noexec option set on /tmp partition	<p>Description</p> <p>The noexec mount option specifies that the filesystem cannot contain executable binaries.</p>

	<p>Rationale</p> <p>Since the /tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from /tmp .</p>
1.1.8 Ensure nodev option set on /var/tmp partition	<p>Description</p> <p>The nodev mount option specifies that the filesystem cannot contain special devices.</p> <p>Rationale</p> <p>Since the /var/tmp filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices in /var/tmp .</p>
1.1.9 Ensure nosuid option set on /var/tmp partition	<p>Description</p> <p>The nosuid mount option specifies that the filesystem cannot contain setuid files.</p> <p>Rationale</p> <p>Since the /var/tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot create setuid files in /var/tmp .</p>
1.1.10 Ensure noexec option set on /var/tmp partition	<p>Description</p> <p>The noexec mount option specifies that the filesystem cannot contain executable binaries.</p>

	<p>Rationale</p> <p>Since the /var/tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot run executable binaries from /var/tmp .</p>
1.1.14 Ensure nodev option set on /home partition	<p>Description</p> <p>The nodev mount option specifies that the filesystem cannot contain special devices.</p> <p>Rationale</p> <p>Since the user partitions are not intended to support devices, set this option to ensure that users cannot attempt to create block or character special devices.</p>
1.1.15 Ensure nodev option set on /dev/shm partition	<p>Description</p> <p>The nodev mount option specifies that the filesystem cannot contain special devices.</p> <p>Rationale</p> <p>Since the /dev/shm filesystem is not intended to support devices, set this option to ensure that users cannot attempt to create special devices in /dev/shm partitions.</p>
1.1.16 Ensure nosuid option set on /dev/shm partition	<p>Description</p> <p>The nosuid mount option specifies that the filesystem cannot contain setuid files.</p>

	<p>Rationale</p> <p>Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.</p>
1.2.3 Ensure gpgcheck is globally activated	<p>Description</p> <p>The gpgcheck option, found in the main section of the /etc/yum.conf and individual /etc/yum/repos.d/* files determines if an RPM package's signature is checked prior to its installation.</p> <p>Rationale</p> <p>It is important to ensure that an RPM's package signature is always checked prior to installation to ensure that the software is obtained from a trusted source.</p>
1.4.1 Ensure permissions on bootloader config are configured	<p>Description</p> <p>The grub configuration file contains information on boot settings and passwords for unlocking boot options. The grub configuration is usually located at /boot/grub2/grub.cfg and linked as /etc/grub2.cfg. Additional settings can be found in the /boot/grub2/user.cfg file.</p> <p>Rationale</p> <p>Setting the permissions to read and write for root only prevents non-root users from seeing the boot parameters or changing them. Non-root users who read the boot parameters may be able to identify weaknesses in security upon boot and be able to exploit them.</p>

<p>1.4.2 Ensure authentication required for single user mode</p>	<p>Description</p> <p>Single user mode (rescue mode) is used for recovery when the system detects an issue during boot or by manual selection from the bootloader.</p> <p>Rationale</p> <p>Requiring authentication in single user mode (rescue mode) prevents an unauthorized user from rebooting the system into single user to gain root privileges without credentials.</p>
<p>1.5.3 Ensure prelink is disabled</p>	<p>Description</p> <p>prelink is a program that modifies ELF shared libraries and ELF dynamically linked binaries in such a way that the time needed for the dynamic linker to perform relocations at startup significantly decreases.</p> <p>Rationale</p> <p>The prelinking feature can interfere with the operation of AIDE, because it changes binaries. Prelinking can also increase the vulnerability of the system if a malicious user is able to compromise a common library such as libc.</p>
<p>1.6.2 Ensure SELinux is installed</p>	<p>Description</p> <p>SELinux provides Mandatory Access Controls.</p> <p>Rationale</p>

	<p>Without a Mandatory Access Control system installed only the default Discretionary Access Control system will be available.</p>
1.6.1.1 Ensure SELinux is not disabled in bootloader configuration	<p>Description</p> <p>Configure SELINUX to be enabled at boot time and verify that it has not been overwritten by the grub boot parameters.</p> <p>Rationale</p> <p>SELinux must be enabled at boot time in your grub configuration to ensure that the controls it provides are not overridden.</p>
1.6.1.4 Ensure SETroubleshoot is not installed	<p>Description</p> <p>The SETroubleshoot service notifies desktop users of SELinux denials through a user-friendly interface. The service provides important information around configuration errors, unauthorized intrusions, and other potential errors.</p> <p>Rationale</p> <p>The SETroubleshoot service is an unnecessary daemon to have running on a server, especially if X Windows is disabled.</p>
1.6.1.5 Ensure the MCS Translation Service (mcstrans) is not installed	<p>Description</p> <p>The mcstransd daemon provides category label information to client processes requesting information. The label translations are defined in /etc/selinux/targeted/setrans.conf</p>

	<p>Rationale</p> <p>Since this service is not used very often, remove it to reduce the amount of potentially vulnerable code running on the system.</p>
1.7.1.4 Ensure permissions on /etc/motd are configured	<p>Description</p> <p>The contents of the /etc/motd file are displayed to users after login and function as a message of the day for authenticated users.</p> <p>Rationale</p> <p>If the /etc/motd file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.</p>
1.7.1.5 Ensure permissions on /etc/issue are configured	<p>Description</p> <p>The contents of the /etc/issue file are displayed to users prior to login for local terminals.</p> <p>Rationale</p> <p>If the /etc/issue file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.</p>
1.7.1.6 Ensure permissions on /etc/issue.net are configured	<p>Description</p>

	<p>The contents of the /etc/issue.net file are displayed to users prior to login for remote connections from configured services.</p> <p>Rationale</p> <p>If the /etc/issue.net file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.</p>
2.1.2 Ensure X Window System is not installed	<p>Description</p> <p>The X Window System provides a Graphical User Interface (GUI) where users can have multiple windows in which to run programs and various add on. The X Windows system is typically used on workstations where users login, but not on servers where users typically do not login.</p> <p>Rationale</p> <p>Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface.</p>
2.1.15 Ensure mail transfer agent is configured for local-only mode	<p>Description</p> <p>Mail Transfer Agents (MTA), such as sendmail and Postfix, are used to listen for incoming mail and transfer the messages to the appropriate user or mail server. If the system is not intended to be a mail server, it is recommended that the MTA be configured to only process local mail.</p> <p>Rationale</p>

	<p>The software for all Mail Transfer Agents is complex and most have a long history of security issues. While it is important to ensure that the system can process local mail messages, it is not necessary to have the MTA's daemon listening on a port unless the server is intended to be a mail server that receives and processes mail from other systems.</p>
2.1.1.1 Ensure time synchronization is in use	<p>Description</p> <p>System time should be synchronized between all systems in an environment. This is typically done by establishing an authoritative time server or set of servers and having all systems synchronize their clocks to them.</p> <p>Rationale</p> <p>Time synchronization is important to support time sensitive security mechanisms like Kerberos and also ensures log files have consistent time records across the enterprise, which aids in forensic investigations.</p>
2.1.1.2 Ensure ntp is configured	<p>Description</p> <p>ntp is a daemon which implements the Network Time Protocol (NTP). It is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on NTP can be found at http://www.ntp.org. ntp can be configured to be a client and/or a server.</p> <p>This recommendation only applies if ntp is in use on the system.</p> <p>Rationale</p>

	If ntp is in use on the system proper configuration is vital to ensuring time synchronization is working properly.
2.1.1.3 Ensure chrony is configured	<p>Description</p> <p>chrony is a daemon which implements the Network Time Protocol (NTP) is designed to synchronize system clocks across a variety of systems and use a source that is highly accurate. More information on chrony can be found at http://chrony.tuxfamily.org/. chrony can be configured to be a client and/or a server.</p> <p>Rationale</p> <p>If chrony is in use on the system proper configuration is vital to ensuring time synchronization is working properly.</p> <p>This recommendation only applies if chrony is in use on the system.</p>
2.2.1 Ensure NIS Client is not installed	<p>Description</p> <p>The Network Information Service (NIS), formerly known as Yellow Pages, is a client-server directory service protocol used to distribute system configuration files. The NIS client (ypbnd) was used to bind a machine to an NIS server and receive the distributed configuration files.</p> <p>Rationale</p> <p>The NIS service is inherently an insecure system that has been vulnerable to DOS attacks, buffer overflows and has poor authentication for querying NIS maps. NIS generally has been replaced by such protocols</p>

	<p>as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be removed.</p>
2.2.2 Ensure rsh client is not installed	<p>Description</p> <p>The rsh package contains the client commands for the rsh services.</p> <p>Rationale</p> <p>These legacy clients contain numerous security exposures and have been replaced with the more secure SSH package. Even if the server is removed, it is best to ensure the clients are also removed to prevent users from inadvertently attempting to use these commands and therefore exposing their credentials. Note that removing the rsh package removes the clients for rsh , rcp and rlogin .</p>
2.2.3 Ensure talk client is not installed	<p>Description</p> <p>The talk software makes it possible for users to send and receive messages across systems through a terminal session. The talk client, which allows initialization of talk sessions, is installed by default.</p> <p>Rationale</p> <p>The software presents a security risk as it uses unencrypted protocols for communication.</p>
2.2.4 Ensure telnet client is not installed	<p>Description</p> <p>The telnet package contains the telnet client, which allows users to start connections to other systems via the telnet protocol.</p>

	<p>Rationale</p> <p>The telnet protocol is insecure and unencrypted. The use of an unencrypted transmission medium could allow an unauthorized user to steal credentials. The ssh package provides an encrypted session and stronger security and is included in most Linux distributions.</p>
2.2.5 Ensure LDAP client is not installed	<p>Description</p> <p>The Lightweight Directory Access Protocol (LDAP) was introduced as a replacement for NIS/YP. It is a service that provides a method for looking up information from a central database.</p> <p>Rationale</p> <p>If the system will not need to act as an LDAP client, it is recommended that the software be removed to reduce the potential attack surface.</p>
3.3.1 Ensure TCP Wrappers is installed	<p>Description</p> <p>TCP Wrappers provides a simple access list and standardized logging method for services capable of supporting it. In the past, services that were called from inetd and xinetd supported the use of tcp wrappers. As inetd and xinetd have been falling in disuse, any service that can support tcp wrappers will have the libwrap.so library attached to it.</p> <p>Rationale</p> <p>TCP Wrappers provide a good simple access list mechanism to services that may not have that support built in. It is recommended that all services that can support TCP Wrappers, use it.</p>

3.3.2 Ensure /etc/hosts.allow is configured	<p>Description</p> <p>The /etc/hosts.allow file specifies which IP addresses are permitted to connect to the host. It is intended to be used in conjunction with the /etc/hosts.deny file.</p> <p>Rationale</p> <p>The /etc/hosts.allow file supports access control by IP and helps ensure that only authorized systems can connect to the system.</p>
3.3.4 Ensure permissions on /etc/hosts.allow are configured	<p>Description</p> <p>The /etc/hosts.allow file contains networking information that is used by many applications and therefore must be readable for these applications to operate.</p> <p>Rationale</p> <p>It is critical to ensure that the /etc/hosts.allow file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.</p>
3.3.5 Ensure permissions on /etc/hosts.deny are configured	<p>Description</p> <p>The /etc/hosts.deny file contains network information that is used by many system applications and therefore must be readable for these applications to operate.</p> <p>Rationale</p>

	<p>It is critical to ensure that the /etc/hosts.deny file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.</p>
3.5.3 Ensure iptables is installed	<p>Description</p> <p>iptables allows configuration of the IPv4 tables in the linux kernel and the rules stored within them. Most firewall configuration utilities operate as a front end to iptables.</p> <p>Rationale</p> <p>iptables is required for firewall management and configuration.</p>
4.1.1.1 Ensure audit log storage size is configured	<p>Description</p> <p>Configure the maximum size of the audit log file. Once the log reaches the maximum size, it will be rotated and a new log file will be started.</p> <p>Rationale</p> <p>It is important that an appropriate size is determined for log files so that they do not impact the system and audit data is not lost.</p>
4.2.3 Ensure rsyslog or syslog-ng is installed	<p>Description</p> <p>The rsyslog and syslog-ng software are recommended replacements to the original syslogd daemon which provide improvements over syslogd , such as</p>

	<p>connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server.</p> <p>Rationale</p> <p>The security enhancements of rsyslog and syslog-ng such as connection-oriented (i.e. TCP) transmission of logs, the option to log to database formats, and the encryption of log data en route to a central logging server) justify installing and configuring the package.</p>
4.2.2.1 Ensure syslog-ng service is enabled	<p>Description</p> <p>Once the syslog-ng package is installed it needs to be activated.</p> <p>Rationale</p> <p>If the syslog-ng service is not activated the system may default to the syslod service or lack logging instead.</p>
4.2.2.3 Ensure syslog-ng default file permissions configured	<p>Description</p> <p>syslog-ng will create logfiles that do not already exist on the system. This setting controls what permissions will be applied to these newly created files.</p> <p>Rationale</p> <p>It is important to ensure that log files exist and have the correct permissions to ensure that sensitive syslog-ng data is archived and protected.</p>

<p>5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured</p>	<p>Description</p> <p>The /etc/ssh/sshd_config file contains configuration specifications for sshd. The command below sets the owner and group of the file to root.</p> <p>Rationale</p> <p>The /etc/ssh/sshd_config file needs to be protected from unauthorized changes by non-privileged users.</p>
<p>5.2.3 Ensure permissions on SSH public host key files are configured</p>	<p>Description</p> <p>An SSH public key is one of two files used in SSH public key authentication. In this authentication method, a public key is a key that can be used for verifying digital signatures generated using a corresponding private key. Only a public key that corresponds to a private key will be able to authenticate successfully.</p> <p>Rationale</p> <p>If a public host key file is modified by an unauthorized user, the SSH service may be compromised.</p>
<p>5.3.4 Ensure password hashing algorithm is SHA-512</p>	<p>Description</p> <p>The commands below change password encryption from md5 to sha512 (a much stronger hashing algorithm). All existing accounts will need to perform a password change to upgrade the stored hashes to the new algorithm.</p> <p>Rationale</p>

	<p>The SHA-512 algorithm provides much stronger hashing than MD5, thus providing additional protection to the system by increasing the level of effort for an attacker to successfully determine passwords.</p> <p>Note that these changes only apply to accounts configured on the local system.</p>
5.4.2 Ensure system accounts are non-login	<p>Description</p> <p>There are a number of accounts provided with Amazon Linux 2 that are used to manage applications and are not intended to provide an interactive shell.</p> <p>Rationale</p> <p>It is important to make sure that accounts that are not being used by regular users are prevented from being used to provide an interactive shell. By default Amazon Linux 2 sets the password field for these accounts to an invalid string, but it is also recommended that the shell field in the password file be set to /sbin/nologin . This prevents the account from potentially being used to run any commands. Some built-in accounts use /bin/false which is also acceptable. This prevents the account from potentially being used to run any commands.</p>
5.4.3 Ensure default group for the root account is GID 0	<p>Description</p> <p>The usermod command can be used to specify which group the root user belongs to. This affects permissions of files that are created by the root user.</p> <p>Rationale</p> <p>Using GID 0 for the root account helps prevent root - owned files from accidentally becoming accessible to non-privileged users.</p>

<p>6.1.2 Ensure permissions on /etc/passwd are configured</p>	<p>Description</p> <p>The /etc/passwd file contains user account information that is used by many system utilities and therefore must be readable for these utilities to operate.</p> <p>Rationale</p> <p>It is critical to ensure that the /etc/passwd file is protected from unauthorized write access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.</p>
<p>6.1.3 Ensure permissions on /etc/shadow are configured</p>	<p>Description</p> <p>The /etc/shadow file is used to store the information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.</p> <p>Rationale</p> <p>If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert the user accounts.</p>
<p>6.1.4 Ensure permissions on /etc/group are configured</p>	<p>Description</p> <p>The /etc/group file contains a list of all the valid groups defined in the system. The command below allows read/write access for root and read access for everyone else.</p>

	<p>Rationale</p> <p>The /etc/group file needs to be protected from unauthorized changes by non-privileged users, but needs to be readable as this information is used with many non-privileged programs.</p>
6.1.5 Ensure permissions on /etc/gshadow are configured	<p>Description</p> <p>The /etc/gshadow file is used to store the information about groups that is critical to the security of those accounts, such as the hashed password and other security information.</p> <p>Rationale</p> <p>If attackers can gain read access to the /etc/gshadow file, they can easily run a password cracking program against the hashed password to break it. Other security information that is stored in the /etc/gshadow file (such as group administrators) could also be useful to subvert the group.</p>
6.1.6 Ensure permissions on /etc/passwd- are configured	<p>Description</p> <p>The /etc/passwd- file contains backup user account information.</p> <p>Rationale</p> <p>It is critical to ensure that the /etc/passwd- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.</p>

<p>6.1.7 Ensure permissions on /etc/shadow- are configured</p>	<p>Description</p> <p>The /etc/shadow- file is used to store backup information about user accounts that is critical to the security of those accounts, such as the hashed password and other security information.</p> <p>Rationale</p> <p>It is critical to ensure that the /etc/shadow- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.</p>
<p>6.1.8 Ensure permissions on /etc/group- are configured</p>	<p>Description</p> <p>The /etc/group- file contains a backup list of all the valid groups defined in the system.</p> <p>Rationale</p> <p>It is critical to ensure that the /etc/group- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.</p>
<p>6.1.9 Ensure permissions on /etc/gshadow- are configured</p>	<p>Description</p> <p>The /etc/gshadow- file is used to store backup information about groups that is critical to the security of those accounts, such as the hashed password and other security information.</p> <p>Rationale</p>

	<p>It is critical to ensure that the /etc/gshadow- file is protected from unauthorized access. Although it is protected by default, the file permissions could be changed either inadvertently or through malicious actions.</p>
6.2.2 Ensure no legacy "+" entries exist in /etc/passwd	<p>Description</p> <p>The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.</p> <p>Rationale</p> <p>These entries may provide an avenue for attackers to gain privileged access on the system.</p>
6.2.3 Ensure no legacy "+" entries exist in /etc/shadow	<p>Description</p> <p>The character + in various files used to be markers for systems to insert data from NIS maps at a certain point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.</p> <p>Rationale</p> <p>These entries may provide an avenue for attackers to gain privileged access on the system.</p>
6.2.4 Ensure no legacy "+" entries exist in /etc/group	<p>Description</p> <p>The character + in various files used to be markers for systems to insert data from NIS maps at a certain</p>

	<p>point in a system configuration file. These entries are no longer required on most systems, but may exist in files that have been imported from other platforms.</p> <p>Rationale</p> <p>These entries may provide an avenue for attackers to gain privileged access on the system.</p>
6.2.5 Ensure root is the only UID 0 account	<p>Description</p> <p>Any account with UID 0 has superuser privileges on the system.</p> <p>Rationale</p> <p>This access must be limited to only the default root account and only from the system console. Administrative access must be through an unprivileged account using an approved mechanism as noted in Item 5.6 Ensure access to the su command is restricted.</p>
6.2.6 Ensure root PATH Integrity	<p>Description</p> <p>The root user can execute any command on the system and could be fooled into executing programs unintentionally if the PATH is not set correctly.</p> <p>Rationale</p> <p>Including the current working directory (.) or other writable directory in root's executable path makes it likely that an attacker can gain superuser access by forcing an administrator operating as root to execute a Trojan horse program.</p>

<p>6.2.7 Ensure all users' home directories exist</p>	<p>Description</p> <p>Users can be defined in /etc/passwd without a home directory or with a home directory that does not actually exist.</p> <p>Rationale</p> <p>If the user's home directory does not exist or is unassigned, the user will be placed in "/" and will not be able to write any files or have local environment variables set.</p>
<p>6.2.8 Ensure users' home directories permissions are 750 or more restrictive</p>	<p>Description</p> <p>While the system administrator can establish secure permissions for users' home directories, the users can easily override these.</p> <p>Rationale</p> <p>Group or world-writable user home directories may enable malicious users to steal or modify other users' data or to gain another user's system privileges.</p>
<p>6.2.9 Ensure users own their home directories</p>	<p>Description</p> <p>The user home directory is space defined for the particular user to set local environment variables and to store personal files.</p> <p>Rationale</p>

	<p>Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.</p>
6.2.10 Ensure users' dot files are not group or world writable	<p>Description</p> <p>While the system administrator can establish secure permissions for users' "dot" files, the users can easily override these.</p> <p>Rationale</p> <p>Group or world-writable user configuration files may enable malicious users to steal or modify other users' data or to gain another user's system privileges.</p>
6.2.11 Ensure no users have .forward files	<p>Description</p> <p>The .forward file specifies an email address to forward the user's mail to.</p> <p>Rationale</p> <p>Use of the .forward file poses a security risk in that sensitive data may be inadvertently transferred outside the organization. The .forward file also poses a risk as it can be used to execute commands that may perform unintended actions.</p>
6.2.12 Ensure no users have .netrc files	<p>Description</p> <p>The .netrc file contains data for logging into a remote host for file transfers via FTP.</p> <p>Rationale</p>

	<p>The .netrc file presents a significant security risk since it stores passwords in unencrypted form. Even if FTP is disabled, user accounts may have brought over .netrc files from other systems which could pose a risk to those systems.</p>
6.2.13 Ensure users' .netrc Files are not group or world accessible	<p>Description</p> <p>While the system administrator can establish secure permissions for users' .netrc files, the users can easily override these.</p> <p>Rationale</p> <p>.netrc files may contain unencrypted passwords that may be used to attack other systems.</p>
6.2.14 Ensure no users have .rhosts files	<p>Description</p> <p>While no .rhosts files are shipped by default, users can easily create them.</p> <p>Rationale</p> <p>This action is only meaningful if .rhosts support is permitted in the file /etc/pam.conf . Even though the .rhosts files are ineffective if support is disabled in /etc/pam.conf , they may have been brought over from other systems and could contain information useful to an attacker for those other systems.</p>
6.2.15 Ensure all groups in /etc/passwd exist in /etc/group	<p>Description</p>

	<p>Over time, system administration errors and changes can lead to groups being defined in /etc/passwd but not in /etc/group .</p> <p>Rationale</p> <p>Groups defined in the /etc/passwd file but not in the /etc/group file pose a threat to system security since group permissions are not properly managed.</p>
6.2.16 Ensure no duplicate UIDs exist	<p>Description</p> <p>Although the useradd program will not let you create a duplicate User ID (UID), it is possible for an administrator to manually edit the /etc/passwd file and change the UID field.</p> <p>Rationale</p> <p>Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.</p>
6.2.17 Ensure no duplicate GIDs exist	<p>Description</p> <p>Although the groupadd program will not let you create a duplicate Group ID (GID), it is possible for an administrator to manually edit the /etc/group file and change the GID field.</p> <p>Rationale</p> <p>User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.</p>

6.2.18 Ensure no duplicate user names exist	<p>Description</p> <p>Although the useradd program will not let you create a duplicate user name, it is possible for an administrator to manually edit the /etc/passwd file and change the user name.</p> <p>Rationale</p> <p>If a user is assigned a duplicate user name, it will create and have access to files with the first UID for that username in /etc/passwd . For example, if "test4" has a UID of 1000 and a subsequent "test4" entry has a UID of 2000, logging in as "test4" will use UID 1000. Effectively, the UID is shared, which is a security problem.</p>
6.2.19 Ensure no duplicate group names exist	<p>Description</p> <p>Although the groupadd program will not let you create a duplicate group name, it is possible for an administrator to manually edit the /etc/group file and change the group name.</p> <p>Rationale</p> <p>If a group is assigned a duplicate group name, it will create and have access to files with the first GID for that group in /etc/group . Effectively, the GID is shared, which is a security problem.</p>

5.2 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/webframeclient_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 protocols 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 IFRAAME 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 xsltGenerateId 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 <code>HTMLFormElement::removeFormElement</code> function in <code>html/HTMLFormElement.cpp</code> 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 <code>FrameView::calculateScrollbarModesForLayout</code> function in <code>page/FrameView.cpp</code> 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 <code>removeChild</code> method during interaction with a FRAME element.
CVE-2011-1798	<code>rendering/svg/RenderSVGText.cpp</code> 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	<code>rendering/RenderBox.cpp</code> 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 EA Server 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 Autocomplete 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::executelfJavaScriptURL 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 db2dasrm 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-2013-1369, 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-2013-2139	Buffer overflow in srtp.c in libsrtp in srtp 1.4.5 and earlier allows remote attackers to cause a denial of service (crash) via vectors related to a length inconsistency in the crypto_policy_set_from_profile_for_rtp and srtp_protect functions.
CVE-2013-2268	Unspecified vulnerability in the MathML implementation in WebKit in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, has unknown impact and remote attack vectors, related to a "high severity security issue."
CVE-2013-2503	Privoxy before 3.0.21 does not properly handle Proxy-Authenticate and Proxy-Authorization headers in the client-server data stream, which makes it easier for remote HTTP servers to spoof the intended proxy service via a 407 (aka Proxy Authentication Required) HTTP status code.
CVE-2013-2549	Unspecified vulnerability in Adobe Reader 11.0.02 allows remote attackers to execute arbitrary code via vectors related to a "break into the sandbox," as demonstrated by George Hotz during a Pwn2Own competition at CanSecWest 2013.
CVE-2013-2550	Unspecified vulnerability in Adobe Reader 11.0.02 allows attackers to bypass the sandbox protection mechanism via unknown vectors, as demonstrated by George Hotz during a Pwn2Own competition at CanSecWest 2013.
CVE-2013-2555	Integer overflow in Adobe Flash Player before 10.3.183.75 and 11.x before 11.7.700.169 on Windows and Mac OS X, before 10.3.183.75 and 11.x before 11.2.202.280 on Linux, before 11.1.111.50 on Android 2.x and 3.x, and before 11.1.115.54 on Android 4.x; Adobe AIR before 3.7.0.1530; and Adobe AIR SDK & Compiler before 3.7.0.1530 allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2013.
CVE-2013-2632	Google V8 before 3.17.13, as used in Google Chrome before 27.0.1444.3, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code, as demonstrated by the Bejeweled game.
CVE-2013-2718	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734,

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

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

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

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

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

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

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

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

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

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

	Content) status code, in conjunction with a delay in notifying the user of an attempted spoof.
CVE-2013-2917	The ReverbConvolverStage::ReverbConvolverStage function in core/platform/audio/ReverbConvolverStage.cpp in the Web Audio implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the impulseResponse array.
CVE-2013-2918	Use-after-free vulnerability in the RenderBlock::collapseAnonymousBlockChild function in core/rendering/RenderBlock.cpp in the DOM implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect handling of parent-child relationships for anonymous blocks.
CVE-2013-2919	Google V8, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2920	The DoResolveRelativeHost function in url/url_canon_relative.cc in Google Chrome before 30.0.1599.66 allows remote attackers to cause a denial of service (out-of-bounds read) via a relative URL containing a hostname, as demonstrated by a protocol-relative URL beginning with a //www.google.com/ substring.
CVE-2013-2921	Double free vulnerability in the ResourceFetcher::didLoadResource function in core/fetch/ResourceFetcher.cpp in the resource loader in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering certain callback processing during the reporting of a resource entry.
CVE-2013-2922	Use-after-free vulnerability in core/html/HTMLElementTemplate.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-2013-5211	The monlist feature in ntp_request.c in ntpd in NTP before 4.2.7p26 allows remote attackers to cause a denial of service (traffic amplification) via forged (1) REQ_MON_GETLIST or (2) REQ_MON_GETLIST_1 requests, as exploited in the wild in December 2013.
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/tgload.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-2014-3634	rsyslog before 7.6.6 and 8.x before 8.4.1 and sysklogd 1.5 and earlier allows remote attackers to cause a denial of service (crash), possibly execute arbitrary code, or have other unspecified impact via a crafted priority (PRI) value that triggers an out-of-bounds array access.
CVE-2014-3803	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-2014-4617	The do_uncompress function in g10/compress.c in GnuPG 1.x before 1.4.17 and 2.x before 2.0.24 allows context-dependent attackers to cause a denial of service (infinite loop) via malformed compressed packets, as demonstrated by an a3 01 5b ff byte sequence.
CVE-2014-4671	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-2014-6272	Multiple integer overflows in the evbuffer API in Libevent 1.4.x before 1.4.15, 2.0.x before 2.0.22, and 2.1.x before 2.1.5-beta allow context-dependent attackers to cause a denial of service or possibly have other unspecified impact via "insanely large inputs" to the (1) evbuffer_add, (2) evbuffer_expand, or (3) bufferevent_write function, which triggers a heap-based buffer overflow or an infinite loop. NOTE: this identifier has been SPLIT per ADT3 due to different affected versions. See CVE-2015-6525 for the functions that are only affected in 2.0 and later.
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-2014-8583	mod_wsgi before 4.2.4 for Apache, when creating a daemon process group, does not properly handle when

	group privileges cannot be dropped, which might allow attackers to gain privileges via unspecified vectors.
CVE-2014-9162	Adobe Flash Player before 13.0.0.259 and 14.x through 16.x before 16.0.0.235 on Windows and OS X and before 11.2.202.425 on Linux allows attackers to obtain sensitive information via unspecified vectors.
CVE-2014-9163	Stack-based buffer overflow in Adobe Flash Player before 13.0.0.259 and 14.x and 15.x before 15.0.0.246 on Windows and OS X and before 11.2.202.425 on Linux allows attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in December 2014.
CVE-2014-9164	Adobe Flash Player before 13.0.0.259 and 14.x through 16.x before 16.0.0.235 on Windows and OS X and before 11.2.202.425 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0587.
CVE-2014-9646	Unquoted Windows search path vulnerability in the GoogleChromeDistribution::DoPostUninstallOperations function in installer/util/google_chrome_distribution.cc in the uninstall-survey feature in Google Chrome before 40.0.2214.91 allows local users to gain privileges via a Trojan horse program in the %SYSTEMDRIVE% directory, as demonstrated by program.exe, a different vulnerability than CVE-2015-1205.
CVE-2014-9647	Use-after-free vulnerability in PDFium, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document, related to fpdfsdk/src/fpdfview.cpp and fpdfsdk/src/fsdk_mngr.cpp, a different vulnerability than CVE-2015-1205.
CVE-2014-9654	The Regular Expressions package in International Components for Unicode (ICU) for C/C++ before 2014-12-03, as used in Google Chrome before 40.0.2214.91, calculates certain values without ensuring that they can be represented in a 24-bit field, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted string, a related issue to CVE-2014-7923.
CVE-2014-9689	content/renderer/device_sensors/device_orientation_event_pump.cc in Google Chrome before 41.0.2272.76 does not properly restrict access to high-rate gyroscope data, which makes it easier for remote attackers to obtain speech signals from a device's physical environment via a crafted web site that listens for ondeviceorientation events, a different vulnerability than CVE-2015-1231.

CVE-2015-0225	The default configuration in Apache Cassandra 1.2.0 through 1.2.19, 2.0.0 through 2.0.13, and 2.1.0 through 2.1.3 binds an unauthenticated JMX/RMI interface to all network interfaces, which allows remote attackers to execute arbitrary Java code via an RMI request.
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/FECColorMatrix.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::updateTimingInfoForFrameNavigation 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-2015-1819	The xmlreader in libxml allows remote attackers to cause a denial of service (memory consumption) via crafted XML data, related to an XML Entity Expansion (XEE) attack.
CVE-2015-2238	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-2015-5312	The xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.3 does not properly prevent entity expansion, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted XML data, a different vulnerability than CVE-2014-3660.
CVE-2015-5377	** 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-2015-6360	The encryption-processing feature in Cisco libSRTP before 1.5.3 allows remote attackers to cause a denial of service via crafted fields in SRTP packets, aka Bug ID CSCux00686.
CVE-2015-6525	Multiple integer overflows in the evbuffer API in Libevent 2.0.x before 2.0.22 and 2.1.x before 2.1.5-beta allow context-dependent attackers to cause a denial of service or possibly have other unspecified impact via "insanely large inputs" to the (1) evbuffer_add, (2) evbuffer_prepend, (3) evbuffer_expand, (4) evbuffer_reserve_space, or (5) evbuffer_read function, which triggers a heap-based buffer overflow or an infinite loop. NOTE: this identifier was SPLIT from CVE-2014-6272 per ADT3 due to different affected versions.
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-2015-7497	Heap-based buffer overflow in the xmlDictComputeFastQKey function in dict.c in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service via unspecified vectors.
CVE-2015-7498	Heap-based buffer overflow in the xmlParseXmlDecl function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service via unspecified vectors related to extracting errors after an encoding conversion failure.
CVE-2015-7499	Heap-based buffer overflow in the xmlGROW function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to obtain sensitive process memory information via unspecified vectors.
CVE-2015-7500	The xmlParseMisc function in parser.c in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service (out-of-bounds heap read) via unspecified vectors related to incorrect entities boundaries and start tags.
CVE-2015-7625	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-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7697	Info-ZIP UnZip 6.0 allows remote attackers to cause a denial of service (infinite loop) via empty bzip2 data in a ZIP archive.

CVE-2015-7834	Multiple unspecified vulnerabilities in Google V8 before 4.6.85.23, as used in Google Chrome before 46.0.2490.71, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-7941	libxml2 2.9.2 does not properly stop parsing invalid input, which allows context-dependent attackers to cause a denial of service (out-of-bounds read and libxml2 crash) via crafted XML data to the (1) xmlParseEntityDecl or (2) xmlParseConditionalSections function in parser.c, as demonstrated by non-terminated entities.
CVE-2015-7942	The xmlParseConditionalSections function in parser.c in libxml2 does not properly skip intermediary entities when it stops parsing invalid input, which allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via crafted XML data, a different vulnerability than CVE-2015-7941.
CVE-2015-8035	The xz_decomp function in xzlib.c in libxml2 2.9.1 does not properly detect compression errors, which allows context-dependent attackers to cause a denial of service (process hang) via crafted XML data.
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-2015-8241	The xmlNextChar function in libxml2 2.9.2 does not properly check the state, which allows context-dependent attackers to cause a denial of service (heap-based buffer over-read and application crash) or obtain sensitive information via crafted XML data.
CVE-2015-8242	The xmlSAX2TextNode function in SAX2.c in the push interface in the HTML parser in libxml2 before 2.9.3 allows context-dependent attackers to cause a denial of service (stack-based buffer over-read and application crash) or obtain sensitive information via crafted XML data.

CVE-2015-8317	The <code>xmlParseXMLDecl</code> function in <code>parser.c</code> in <code>libxml2</code> before 2.9.3 allows context-dependent attackers to obtain sensitive information via an (1) unterminated encoding value or (2) incomplete XML declaration in XML data, which triggers an out-of-bounds heap read.
CVE-2015-8401	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 <code>toString</code> 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 <code>getRemote</code> 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-2015-8710	The htmlParseComment function in HTMLparser.c in libxml2 allows attackers to obtain sensitive information, cause a denial of service (out-of-bounds heap memory access and application crash), or possibly have unspecified other impact via an unclosed HTML comment.
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-2015-9251	jQuery before 3.0.0 is vulnerable to Cross-site Scripting (XSS) attacks when a cross-domain Ajax request is performed without the dataType option, causing text/javascript responses to be executed.
CVE-2015-9262	_XcursorThemeInherits in library.c in libXcursor before 1.1.15 allows remote attackers to cause denial of service or potentially code execution via a one-byte heap overflow.
CVE-2016-0959	Use after free vulnerability in Adobe Flash Player Desktop Runtime before 20.0.0.267, Adobe Flash

	Player Extended Support Release before 18.0.0.324, Adobe Flash Player for Google Chrome before 20.0.0.267, Adobe Flash Player for Microsoft Edge and Internet Explorer 11 before 20.0.0.267, Adobe Flash Player for Internet Explorer 10 and 11 before 20.0.0.267, Adobe Flash Player for Linux before 11.2.202.559, AIR Desktop Runtime before 20.0.0.233, AIR SDK before 20.0.0.233, AIR SDK & Compiler before 20.0.0.233, AIR for Android before 20.0.0.233.
CVE-2016-0960	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.
CVE-2016-0961	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.
CVE-2016-0962	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.
CVE-2016-0963	Integer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0993 and CVE-2016-1010.

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

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

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

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

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

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

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

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

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

	CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, and CVE-2016-1002.
CVE-2016-1006	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to bypass the ASLR protection mechanism via JIT data.
CVE-2016-1010	Integer overflow in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0963 and CVE-2016-0993.
CVE-2016-1011	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1013, CVE-2016-1016, CVE-2016-1017, and CVE-2016-1031.
CVE-2016-1012	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1013	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1011, CVE-2016-1016, CVE-2016-1017, and CVE-2016-1031.
CVE-2016-1014	Untrusted search path vulnerability in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows local users to gain privileges via a Trojan horse resource in an unspecified directory.
CVE-2016-1015	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code by overriding NetConnection object properties to leverage an

	unspecified "type confusion," a different vulnerability than CVE-2016-1019.
CVE-2016-1016	Use-after-free vulnerability in the Transform object implementation in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via a flash.geom.Matrix callback, a different vulnerability than CVE-2016-1011, CVE-2016-1013, CVE-2016-1017, and CVE-2016-1031.
CVE-2016-1017	Use-after-free vulnerability in the LoadVars.decode function in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1011, CVE-2016-1013, CVE-2016-1016, and CVE-2016-1031.
CVE-2016-1018	Stack-based buffer overflow in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via crafted JPEG-XR data.
CVE-2016-1019	Adobe Flash Player 21.0.0.197 and earlier allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unspecified vectors, as exploited in the wild in April 2016.
CVE-2016-1020	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1021	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1022	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to

	execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-10228	The iconv program in the GNU C Library (aka glibc or libc6) 2.31 and earlier, when invoked with multiple suffixes in the destination encoding (TRANSLATE or IGNORE) along with the -c option, enters an infinite loop when processing invalid multi-byte input sequences, leading to a denial of service.
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-2016-10245	Insufficient sanitization of the query parameter in templates/html/search_opensearch.php could lead to reflected cross-site scripting or iframe injection.
CVE-2016-1025	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1026	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different

	vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1027	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1028	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1029	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1030	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to bypass intended access restrictions via unspecified vectors.
CVE-2016-1031	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-1011, CVE-2016-1013, CVE-2016-1016, and CVE-2016-1017.
CVE-2016-1032	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service

	(memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, and CVE-2016-1033.
CVE-2016-1033	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, and CVE-2016-1032.
CVE-2016-10713	An issue was discovered in GNU patch before 2.7.6. Out-of-bounds access within pch_write_line() in pch.c can possibly lead to DoS via a crafted input file.
CVE-2016-10735	In Bootstrap 3.x before 3.4.0 and 4.x-beta before 4.0.0-beta.2, XSS is possible in the data-target attribute, a different vulnerability than CVE-2018-14041.
CVE-2016-10739	In the GNU C Library (aka glibc or libc6) through 2.28, the getaddrinfo function would successfully parse a string that contained an IPv4 address followed by whitespace and arbitrary characters, which could lead applications to incorrectly assume that it had parsed a valid string, without the possibility of embedded HTTP headers or other potentially dangerous substrings.
CVE-2016-10745	In Pallets Jinja before 2.8.1, str.format allows a sandbox escape.
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::RequireForJSLInner 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 Autocomplete 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-2016-2124	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.
CVE-2016-2191	The bmp_read_rows function in pngxtern/pngxbmp.c in OptiPNG before 0.7.6 allows remote attackers to cause a denial of service (invalid memory write and crash) via a series of delta escapes in a crafted BMP image.
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-2016-3186	Buffer overflow in the readextension function in gif2tiff.c in LibTIFF 4.0.6 allows remote attackers to cause a

	denial of service (application crash) via a crafted GIF file.
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-2016-4463	Stack-based buffer overflow in Apache Xerces-C++ before 3.1.4 allows context-dependent attackers to cause a denial of service via a deeply nested DTD.
CVE-2016-4658	xpointer.c in libxml2 before 2.9.5 (as used in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3, and other products) does not forbid namespace nodes in XPointer ranges, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and memory corruption) via a crafted XML document.

CVE-2016-5003	The Apache XML-RPC (aka ws-xmlrpc) library 3.1.3, as used in Apache Archiva, allows remote attackers to execute arbitrary code via a crafted serialized Java object in an <ex:serializable> element.
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_FormFilter::KillFocusForAnnot, which allowed a remote attacker to potentially exploit heap corruption via crafted PDF files.

CVE-2016-5185	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly allowed reentrance of FrameView::updateLifecyclePhasesInternal(), which allowed a remote attacker to perform an out of bounds memory read via crafted HTML pages.
CVE-2016-5186	Devtools in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled objects after a tab crash, which allowed a remote attacker to perform an out of bounds memory read via crafted PDF files.
CVE-2016-5187	Google Chrome prior to 54.0.2840.85 for Android incorrectly handled rapid transition into and out of full screen mode, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages.
CVE-2016-5188	Multiple issues in Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux allow a remote attacker to spoof various parts of browser UI via crafted HTML pages.
CVE-2016-5189	Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android permitted navigation to blob URLs with non-canonical origins, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages.
CVE-2016-5190	Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object lifecycles during shutdown, which allowed a remote attacker to perform an out of bounds memory read via crafted HTML pages.
CVE-2016-5191	Bookmark handling in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android had insufficient validation of supplied data, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages, as demonstrated by an interpretation conflict between userinfo and scheme in an http://javascript:payload@example.com URL.
CVE-2016-5192	Blink in Google Chrome prior to 54.0.2840.59 for Windows missed a CORS check on redirect in TextTrackLoader, which allowed a remote attacker to bypass cross-origin restrictions via crafted HTML pages.
CVE-2016-5193	Google Chrome prior to 54.0 for iOS had insufficient validation of URLs for windows open by DOM, which allowed a remote attacker to bypass restrictions on navigation to certain URL schemes via crafted HTML pages.

CVE-2016-5194	Unspecified vulnerabilities in Google Chrome before 54.0.2840.59.
CVE-2016-5198	V8 in Google Chrome prior to 54.0.2840.90 for Linux, and 54.0.2840.85 for Android, and 54.0.2840.87 for Windows and Mac included incorrect optimisation assumptions, which allowed a remote attacker to perform arbitrary read/write operations, leading to code execution, via a crafted HTML page.
CVE-2016-5199	An off by one error resulting in an allocation of zero size in FFmpeg in Google Chrome prior to 54.0.2840.98 for Mac, and 54.0.2840.99 for Windows, and 54.0.2840.100 for Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2016-5200	V8 in Google Chrome prior to 54.0.2840.98 for Mac, and 54.0.2840.99 for Windows, and 54.0.2840.100 for Linux, and 55.0.2883.84 for Android incorrectly applied type rules, which allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5201	A leak of privateClass in the extensions API in Google Chrome prior to 54.0.2840.100 for Linux, and 54.0.2840.99 for Windows, and 54.0.2840.98 for Mac allowed a remote attacker to access privileged JavaScript code via a crafted HTML page.
CVE-2016-5202	browser/extensions/api/dial/dial_registry.cc in Google Chrome before 54.0.2840.98 on macOS, before 54.0.2840.99 on Windows, and before 54.0.2840.100 on Linux neglects to copy a device ID before an erase() call, which causes the erase operation to access data that that erase operation will destroy.
CVE-2016-5203	A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2016-5204	Leaking of an SVG shadow tree leading to corruption of the DOM tree in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2016-5205	Blink in Google Chrome prior to 55.0.2883.75 for Linux, Windows and Mac, incorrectly handles deferred page loads, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2016-5206	The PDF plugin in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly followed redirects,

	which allowed a remote attacker to bypass the Same Origin Policy via a crafted HTML page.
CVE-2016-5207	In Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android, corruption of the DOM tree could occur during the removal of a full screen element, which allowed a remote attacker to achieve arbitrary code execution via a crafted HTML page.
CVE-2016-5208	Blink in Google Chrome prior to 55.0.2883.75 for Linux and Windows, and 55.0.2883.84 for Android allowed possible corruption of the DOM tree during synchronous event handling, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2016-5209	Bad casting in bitmap manipulation in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5210	Heap buffer overflow during TIFF image parsing in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2016-5211	A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2016-5212	Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android insufficiently sanitized DevTools URLs, which allowed a remote attacker to read local files via a crafted HTML page.
CVE-2016-5213	A use after free in V8 in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5214	Google Chrome prior to 55.0.2883.75 for Windows mishandled downloaded files, which allowed a remote attacker to prevent the downloaded file from receiving the Mark of the Web via a crafted HTML page.
CVE-2016-5215	A use after free in webaudio in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2016-5216	A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to

	perform an out of bounds memory read via a crafted PDF file.
CVE-2016-5217	The extensions API in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly permitted access to privileged plugins, which allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2016-5218	The extensions API in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled navigation within PDFs, which allowed a remote attacker to temporarily spoof the contents of the Omnibox (URL bar) via a crafted HTML page containing PDF data.
CVE-2016-5219	A heap use after free in V8 in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5220	PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled navigation within PDFs, which allowed a remote attacker to read local files via a crafted PDF file.
CVE-2016-5221	Type confusion in libGLESv2 in ANGLE in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android possibly allowed a remote attacker to bypass buffer validation via a crafted HTML page.
CVE-2016-5222	Incorrect handling of invalid URLs in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2016-5223	Integer overflow in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption or DoS via a crafted PDF file.
CVE-2016-5224	A timing attack on denormalized floating point arithmetic in SVG filters in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to bypass the Same Origin Policy via a crafted HTML page.
CVE-2016-5225	Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled form actions, which allowed a remote attacker to bypass Content Security Policy via a crafted HTML page.

CVE-2016-5226	Blink in Google Chrome prior to 55.0.2883.75 for Linux, Windows and Mac executed javascript: URLs entered in the URL bar in the context of the current tab, which allowed a socially engineered user to XSS themselves by dragging and dropping a javascript: URL into the URL bar.
CVE-2016-5766	Integer overflow in the _gd2GetHeader function in gd_gd2.c in the GD Graphics Library (aka libgd) before 2.2.3, as used in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via crafted chunk dimensions in an image.
CVE-2016-6893	Cross-site request forgery (CSRF) vulnerability in the user options page in GNU Mailman 2.1.x before 2.1.23 allows remote attackers to hijack the authentication of arbitrary users for requests that modify an option, as demonstrated by gaining access to the credentials of a victim's account.
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-2016-7426	NTP before 4.2.8p9 rate limits responses received from the configured sources when rate limiting for all associations is enabled, which allows remote attackers to cause a denial of service (prevent responses from the sources) by sending responses with a spoofed source address.
CVE-2016-7429	NTP before 4.2.8p9 changes the peer structure to the interface it receives the response from a source, which allows remote attackers to cause a denial of service (prevent communication with a source) by sending a response for a source to an interface the source does not use.
CVE-2016-7433	NTP before 4.2.8p9 does not properly perform the initial sync calculations, which allows remote attackers to unspecified impact via unknown vectors, related to a "root distance that did not include the peer dispersion."
CVE-2016-7549	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 <code>render_frame_host_impl.cc</code> and <code>render_widget_host_impl.cc</code> , 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-2016-9310	The control mode (mode 6) functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to set or unset traps via a crafted control mode packet.
CVE-2016-9311	ntpd in NTP before 4.2.8p9, when the trap service is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted packet.
CVE-2016-9396	The JPC_NOMINALGAIN function in jpc/jpc_t1cod.c in JasPer through 2.0.12 allows remote attackers to cause a denial of service (JPC_COX_RFT assertion failure) via unspecified vectors.
CVE-2016-9532	Integer overflow in the writeBufferToSeparateStrips function in tiffcrop.c in LibTIFF before 4.0.7 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted tif file.
CVE-2016-9650	Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled iframes, which allowed a remote attacker to bypass a no-referrer policy via a crafted HTML page.
CVE-2016-9651	A missing check for whether a property of a JS object is private in V8 in Google Chrome prior to 55.0.2883.75 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2016-9652	Multiple unspecified vulnerabilities in Google Chrome before 55.0.2883.75.
CVE-2016-9843	The crc32_big function in crc32.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving big-endian CRC calculation.
CVE-2016-9844	Buffer overflow in the zi_short function in zipinfo.c in Info-Zip UnZip 6.0 allows remote attackers to cause a denial of service (crash) via a large compression method value in the central directory file header.
CVE-2017-0393	A denial of service vulnerability in libvpx in Mediaserver could enable a remote attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High due to the possibility of remote denial of service. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1. Android ID: A-30436808.
CVE-2017-1000050	JasPer 2.0.12 is vulnerable to a NULL pointer exception in the function jp2_encode which failed to check to see if the image contained at least one component resulting in a denial-of-service.

CVE-2017-1000242	Jenkins Git Client Plugin 2.4.2 and earlier creates temporary file with insecure permissions resulting in information disclosure
CVE-2017-1000254	libcurl may read outside of a heap allocated buffer when doing FTP. When libcurl connects to an FTP server and successfully logs in (anonymous or not), it asks the server for the current directory with the 'PWD' command. The server then responds with a 257 response containing the path, inside double quotes. The returned path name is then kept by libcurl for subsequent uses. Due to a flaw in the string parser for this directory name, a directory name passed like this but without a closing double quote would lead to libcurl not adding a trailing NUL byte to the buffer holding the name. When libcurl would then later access the string, it could read beyond the allocated heap buffer and crash or wrongly access data beyond the buffer, thinking it was part of the path. A malicious server could abuse this fact and effectively prevent libcurl-based clients to work with it - the PWD command is always issued on new FTP connections and the mistake has a high chance of causing a segfault. The simple fact that this has issue remained undiscovered for this long could suggest that malformed PWD responses are rare in benign servers. We are not aware of any exploit of this flaw. This bug was introduced in commit [415d2e7cb7] (https://github.com/curl/curl/commit/415d2e7cb7), March 2005. In libcurl version 7.56.0, the parser always zero terminates the string but also rejects it if not terminated properly with a final double quote.
CVE-2017-1000257	An IMAP FETCH response line indicates the size of the returned data, in number of bytes. When that response says the data is zero bytes, libcurl would pass on that (non-existing) data with a pointer and the size (zero) to the deliver-data function. libcurl's deliver-data function treats zero as a magic number and invokes strlen() on the data to figure out the length. The strlen() is called on a heap based buffer that might not be zero terminated so libcurl might read beyond the end of it into whatever memory lies after (or just crash) and then deliver that to the application as if it was actually downloaded.
CVE-2017-1000367	Todd Miller's sudo version 1.8.20 and earlier is vulnerable to an input validation (embedded spaces) in the get_process_ttyname() function resulting in information disclosure and command execution.
CVE-2017-1000368	Todd Miller's sudo version 1.8.20p1 and earlier is vulnerable to an input validation (embedded newlines) in the get_process_ttyname() function resulting in information disclosure and command execution.
CVE-2017-1000405	The Linux Kernel versions 2.6.38 through 4.14 have a problematic use of pmd_mkdirty() in the touch_pmd()

	<p>function inside the THP implementation. touch_pmd() can be reached by get_user_pages(). In such case, the pmd will become dirty. This scenario breaks the new can_follow_write_pmd()'s logic - pmd can become dirty without going through a COW cycle. This bug is not as severe as the original "Dirty cow" because an ext4 file (or any other regular file) cannot be mapped using THP. Nevertheless, it does allow us to overwrite read-only huge pages. For example, the zero huge page and sealed shmem files can be overwritten (since their mapping can be populated using THP). Note that after the first write page-fault to the zero page, it will be replaced with a new fresh (and zeroed) thp.</p>
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-2017-10268	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.19 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).
CVE-2017-10378	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.11 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-10379	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.19 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts).

	CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).
CVE-2017-10384	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.57 and earlier 5.6.37 and earlier 5.7.19 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-10684	In ncurses 6.0, there is a stack-based buffer overflow in the fmt_entry function. A crafted input will lead to a remote arbitrary code execution attack.
CVE-2017-10685	In ncurses 6.0, there is a format string vulnerability in the fmt_entry function. A crafted input will lead to a remote arbitrary code execution attack.
CVE-2017-11112	In ncurses 6.0, there is an attempted 0xfffffffffffffff access in the append_acs function of tinfo/parse_entry.c. It could lead to a remote denial of service attack if the terminfo library code is used to process untrusted terminfo data.
CVE-2017-11113	In ncurses 6.0, there is a NULL Pointer Dereference in the _nc_parse_entry function of tinfo/parse_entry.c. It could lead to a remote denial of service attack if the terminfo library code is used to process untrusted terminfo data.
CVE-2017-11166	The ReadXWDImage function in coders\xwd.c in ImageMagick 7.0.5-6 has a memory leak vulnerability that can cause memory exhaustion via a crafted length (number of color-map entries) field in the header of an XWD file.
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-2017-11368	In MIT Kerberos 5 (aka krb5) 1.7 and later, an authenticated attacker can cause a KDC assertion failure by sending invalid S4U2Self or S4U2Proxy requests.
CVE-2017-12448	The bfd_cache_close function in bfd/cache.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause a heap use after free and possibly achieve code execution via a crafted nested archive file. This issue occurs because incorrect functions are called during an attempt to release memory. The issue can be addressed by better input validation in the bfd_generic_archive_p function in bfd/archive.c.
CVE-2017-12449	The _bfd_vms_save_sized_string function in vms-misc.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms file.
CVE-2017-12450	The alpha_vms_object_p function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap write

	and possibly achieve code execution via a crafted vms alpha file.
CVE-2017-12451	The _bfd_xcoff_read_ar_hdr function in bfd/coff-rs6000.c and bfd/coff64-rs6000.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds stack read via a crafted COFF image file.
CVE-2017-12452	The bfd_mach_o_i386_canonicalize_one_reloc function in bfd/mach-o-i386.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted mach-o file.
CVE-2017-12453	The _bfd_vms_slurp_eeom function in libbfd.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms alpha file.
CVE-2017-12454	The _bfd_vms_slurp_egsd function in bfd/vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an arbitrary memory read via a crafted vms alpha file.
CVE-2017-12455	The evax_bfd_print_emh function in vms-alpha.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted vms alpha file.
CVE-2017-12456	The read_symbol_stabs_debugging_info function in rddb.c in GNU Binutils 2.29 and earlier allows remote attackers to cause an out of bounds heap read via a crafted binary file.
CVE-2017-12457	The bfd_make_section_with_flags function in section.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause a NULL dereference via a crafted file.
CVE-2017-12458	The nlm_swap_auxiliary_headers_in function in bfd/nlmcode.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap read via a crafted nlm file.
CVE-2017-12459	The bfd_mach_o_read_symtab_strtab function in bfd/mach-o.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29 and earlier, allows remote attackers to cause an out of bounds heap write and possibly achieve code execution via a crafted mach-o file.

CVE-2017-12546	A local buffer overflow vulnerability in HPE System Management Homepage for Windows and Linux version prior to v7.6.1 was found.
CVE-2017-12635	Due to differences in the Erlang-based JSON parser and JavaScript-based JSON parser, it is possible in Apache CouchDB before 1.7.0 and 2.x before 2.1.1 to submit _users documents with duplicate keys for 'roles' used for access control within the database, including the special case '_admin' role, that denotes administrative users. In combination with CVE-2017-12636 (Remote Code Execution), this can be used to give non-admin users access to arbitrary shell commands on the server as the database system user. The JSON parser differences result in behaviour that if two 'roles' keys are available in the JSON, the second one will be used for authorising the document write, but the first 'roles' key is used for subsequent authorization for the newly created user. By design, users can not assign themselves roles. The vulnerability allows non-admin users to give themselves admin privileges.
CVE-2017-12636	CouchDB administrative users can configure the database server via HTTP(S). Some of the configuration options include paths for operating system-level binaries that are subsequently launched by CouchDB. This allows an admin user in Apache CouchDB before 1.7.0 and 2.x before 2.1.1 to execute arbitrary shell commands as the CouchDB user, including downloading and executing scripts from the public internet.
CVE-2017-12652	libpng before 1.6.32 does not properly check the length of chunks against the user limit.
CVE-2017-12805	In ImageMagick 7.0.6-6, a memory exhaustion vulnerability was found in the function ReadTIFFImage, which allows attackers to cause a denial of service.
CVE-2017-12806	In ImageMagick 7.0.6-6, a memory exhaustion vulnerability was found in the function format8BIM, which allows attackers to cause a denial of service.
CVE-2017-13194	A vulnerability in the Android media framework (libvpx) related to odd frame width. Product: Android. Versions: 7.0, 7.1.1, 7.1.2, 8.0, 8.1. Android ID: A-64710201.
CVE-2017-13215	A elevation of privilege vulnerability in the Upstream kernel skcipher. Product: Android. Versions: Android kernel. Android ID: A-64386293. References: Upstream kernel.
CVE-2017-13672	QEMU (aka Quick Emulator), when built with the VGA display emulator support, allows local guest OS privileged users to cause a denial of service (out-of-bounds read and QEMU process crash) via vectors involving display update.

CVE-2017-13710	The setup_group function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.29, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a group section that is too small.
CVE-2017-13711	Use-after-free vulnerability in the soffree function in slirp/socket.c in QEMU (aka Quick Emulator) allows attackers to cause a denial of service (QEMU instance crash) by leveraging failure to properly clear ifq_so from pending packets.
CVE-2017-14491	Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS response.
CVE-2017-14492	Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted IPv6 router advertisement request.
CVE-2017-14493	Stack-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DHCPv6 request.
CVE-2017-14494	dnsmasq before 2.78, when configured as a relay, allows remote attackers to obtain sensitive memory information via vectors involving handling DHCPv6 forwarded requests.
CVE-2017-14495	Memory leak in dnsmasq before 2.78, when the --add-mac, --add-cpe-id or --add-subnet option is specified, allows remote attackers to cause a denial of service (memory consumption) via vectors involving DNS response creation.
CVE-2017-14496	Integer underflow in the add_pseudoheader function in dnsmasq before 2.78 , when the --add-mac, --add-cpe-id or --add-subnet option is specified, allows remote attackers to cause a denial of service via a crafted DNS request.
CVE-2017-14503	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-2017-14604	GNOME Nautilus before 3.23.90 allows attackers to spoof a file type by using the .desktop file extension, as demonstrated by an attack in which a .desktop file's Name field ends in .pdf but this file's Exec field launches a malicious "sh -c" command. In other words, Nautilus provides no UI indication that a file actually has the potentially unsafe .desktop extension; instead, the UI only shows the .pdf extension. One (slightly) mitigating factor is that an attack requires the .desktop file to have execute permission. The solution is to

	ask the user to confirm that the file is supposed to be treated as a .desktop file, and then remember the user's answer in the metadata::trusted field.
CVE-2017-14992	Lack of content verification in Docker-CE (Also known as Moby) versions 1.12.6-0, 1.10.3, 17.03.0, 17.03.1, 17.03.2, 17.06.0, 17.06.1, 17.06.2, 17.09.0, and earlier allows a remote attacker to cause a Denial of Service via a crafted image layer payload, aka gzip bombing.
CVE-2017-15041	Go before 1.8.4 and 1.9.x before 1.9.1 allows "go get" remote command execution. Using custom domains, it is possible to arrange things so that example.com/pkg1 points to a Subversion repository but example.com/pkg1/pkg2 points to a Git repository. If the Subversion repository includes a Git checkout in its pkg2 directory and some other work is done to ensure the proper ordering of operations, "go get" can be tricked into reusing this Git checkout for the fetch of code from pkg2. If the Subversion repository's Git checkout has malicious commands in .git/hooks/, they will execute on the system running "go get."
CVE-2017-15042	An unintended cleartext issue exists in Go before 1.8.4 and 1.9.x before 1.9.1. RFC 4954 requires that, during SMTP, the PLAIN auth scheme must only be used on network connections secured with TLS. The original implementation of smtp.PlainAuth in Go 1.0 enforced this requirement, and it was documented to do so. In 2013, upstream issue #5184, this was changed so that the server may decide whether PLAIN is acceptable. The result is that if you set up a man-in-the-middle SMTP server that doesn't advertise STARTTLS and does advertise that PLAIN auth is OK, the smtp.PlainAuth implementation sends the username and password.
CVE-2017-15048	Stack-based buffer overflow in the ZoomLauncher binary in the Zoom client for Linux before 2.0.115900.1201 allows remote attackers to execute arbitrary code by leveraging the zoommtg:// scheme handler.
CVE-2017-15049	The ZoomLauncher binary in the Zoom client for Linux before 2.0.115900.1201 does not properly sanitize user input when constructing a shell command, which allows remote attackers to execute arbitrary code by leveraging the zoommtg:// scheme handler.
CVE-2017-15111	keycloak-htpd-client-install versions before 0.8 insecurely creates temporary file allowing local attackers to overwrite other files via symbolic link.
CVE-2017-15112	keycloak-htpd-client-install versions before 0.8 allow users to insecurely pass password through command line, leaking it via command history and process info to other local users.

CVE-2017-15124	VNC server implementation in Quick Emulator (QEMU) 2.11.0 and older was found to be vulnerable to an unbounded memory allocation issue, as it did not throttle the framebuffer updates sent to its client. If the client did not consume these updates, VNC server allocates growing memory to hold onto this data. A malicious remote VNC client could use this flaw to cause DoS to the server host.
CVE-2017-15131	It was found that system umask policy is not being honored when creating XDG user directories, since Xsession sources xdg-user-dirs.sh before setting umask policy. This only affects xdg-user-dirs before 0.15.5 as shipped with Red Hat Enterprise Linux.
CVE-2017-15134	A stack buffer overflow flaw was found in the way 389-ds-base 1.3.6.x before 1.3.6.13, 1.3.7.x before 1.3.7.9, 1.4.x before 1.4.0.5 handled certain LDAP search filters. A remote, unauthenticated attacker could potentially use this flaw to make ns-slapd crash via a specially crafted LDAP request, thus resulting in denial of service.
CVE-2017-15135	It was found that 389-ds-base since 1.3.6.1 up to and including 1.4.0.3 did not always handle internal hash comparison operations correctly during the authentication process. A remote, unauthenticated attacker could potentially use this flaw to bypass the authentication process under very rare and specific circumstances.
CVE-2017-15268	Qemu through 2.10.0 allows remote attackers to cause a memory leak by triggering slow data-channel read operations, related to io/channel-websock.c.
CVE-2017-15386	Incorrect implementation in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-15387	Insufficient enforcement of Content Security Policy in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to open javascript: URL windows when they should not be allowed to via a crafted HTML page.
CVE-2017-15388	Iteration through non-finite points in Skia in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-15389	An insufficient watchdog timer in navigation in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-15390	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 62.0.3202.62 allowed a remote attacker

	to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-15391	Insufficient Policy Enforcement in Extensions in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to access Extension pages without authorisation via a crafted HTML page.
CVE-2017-15392	Insufficient data validation in V8 in Google Chrome prior to 62.0.3202.62 allowed an attacker who can write to the Windows Registry to potentially exploit heap corruption via a crafted Windows Registry entry, related to PlatformIntegration.
CVE-2017-15393	Insufficient Policy Enforcement in Devtools remote debugging in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to obtain access to remote debugging functionality via a crafted HTML page, aka a Referer leak.
CVE-2017-15394	Insufficient Policy Enforcement in Extensions in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform domain spoofing in permission dialogs via IDN homographs in a crafted Chrome Extension.
CVE-2017-15395	A use after free in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka an ImageCapture NULL pointer dereference.
CVE-2017-15396	A stack buffer overflow in NumberingSystem in International Components for Unicode (ICU) for C/C++ before 60.2, as used in V8 in Google Chrome prior to 62.0.3202.75 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-15398	A stack buffer overflow in the QUIC networking stack in Google Chrome prior to 62.0.3202.89 allowed a remote attacker to gain code execution via a malicious server.
CVE-2017-15399	A use after free in V8 in Google Chrome prior to 62.0.3202.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-15406	A stack buffer overflow in V8 in Google Chrome prior to 62.0.3202.75 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-15407	Out-of-bounds Write in the QUIC networking stack in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to gain code execution via a malicious server.
CVE-2017-15408	Heap buffer overflow in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file that is mishandled by PDFium.
CVE-2017-15409	Heap buffer overflow in Skia in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2017-15410	Use after free in PDFium in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-15411	Use after free in PDFium in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-15412	Use after free in libxml2 before 2.9.5, as used in Google Chrome prior to 63.0.3239.84 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-15413	Type confusion in WebAssembly in V8 in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-15415	Incorrect serialization in IPC in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to leak the value of a pointer via a crafted HTML page.
CVE-2017-15416	Heap buffer overflow in Blob API in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka a Blink out-of-bounds read.
CVE-2017-15417	Inappropriate implementation in Skia canvas composite operations in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2017-15418	Use of uninitialized memory in Skia in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-15419	Insufficient policy enforcement in Resource Timing API in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to infer browsing history by triggering a leaked cross-origin URL via a crafted HTML page.
CVE-2017-15420	Incorrect handling of back navigations in error pages in Navigation in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-15422	Integer overflow in international date handling in International Components for Unicode (ICU) for C/C++ before 60.1, as used in V8 in Google Chrome prior to 63.0.3239.84 and other products, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-15423	Inappropriate implementation in BoringSSL SPAKE2 in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to leak the low-order bits of SHA512(password) by inspecting protocol traffic.
CVE-2017-15424	Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker

	to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-15425	Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-15426	Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-15427	Insufficient policy enforcement in Omnibox in Google Chrome prior to 63.0.3239.84 allowed a socially engineered user to XSS themselves by dragging and dropping a javascript: URL into the URL bar.
CVE-2017-15428	Insufficient data validation in V8 builtins string generator could lead to out of bounds read and write access in V8 in Google Chrome prior to 62.0.3202.94 and allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2017-15429	Inappropriate implementation in V8 WebAssembly JS bindings in Google Chrome prior to 63.0.3239.108 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-15430	Insufficient data validation in Chromecast plugin in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-15670	The GNU C Library (aka glibc or libc6) before 2.27 contains an off-by-one error leading to a heap-based buffer overflow in the glob function in glob.c, related to the processing of home directories using the ~ operator followed by a long string.
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-2017-15804	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27 contains a buffer overflow during unescaping of user names with the ~ operator.
CVE-2017-15906	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
CVE-2017-16931	parser.c in libxml2 before 2.9.5 mishandles parameter-entity references because the NEXTL macro calls the xmlParserHandlePEReference function in the case of a '%' character in a DTD name.
CVE-2017-16939	The XFRM dump policy implementation in net/xfrm/xfrm_user.c in the Linux kernel before 4.13.11 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted SO_RCVBUF setsockopt system call in conjunction with XFRM_MSG_GETPOLICY Netlink messages.
CVE-2017-17724	In Exiv2 0.26, there is a heap-based buffer over-read in the Exiv2::IptcData::printStructure function in iptc.cpp, related to the "!= 0x1c" case. Remote attackers can exploit this vulnerability to cause a denial of service via a crafted TIFF file.
CVE-2017-17741	The KVM implementation in the Linux kernel through 4.14.7 allows attackers to obtain potentially sensitive information from kernel memory, aka a write_mmio stack-based out-of-bounds read, related to arch/x86/kvm/x86.c and include/trace/events/kvm.h.
CVE-2017-17742	Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1 allows an HTTP Response Splitting attack. An attacker can inject a crafted key and value into an HTTP response for the HTTP server of WEBrick.
CVE-2017-17790	The lazy_initialize function in lib/resolv.rb in Ruby through 2.4.3 uses Kernel#open, which might allow Command Injection attacks, as demonstrated by a Resolv::Hosts::new argument beginning with a ' ' character, a different vulnerability than CVE-2017-17405. NOTE: situations with untrusted input may be highly unlikely.
CVE-2017-17833	OpenSLP releases in the 1.0.2 and 1.1.0 code streams have a heap-related memory corruption issue which may manifest itself as a denial-of-service or a remote code-execution vulnerability.
CVE-2017-18189	In the startread function in xa.c in Sound eXchange (SoX) through 14.4.2, a corrupt header specifying zero channels triggers an infinite loop with a resultant NULL

	pointer dereference, which may allow a remote attacker to cause a denial-of-service.
CVE-2017-18190	A localhost.localdomain whitelist entry in valid_host() in scheduler/client.c in CUPS before 2.2.2 allows remote attackers to execute arbitrary IPP commands by sending POST requests to the CUPS daemon in conjunction with DNS rebinding. The localhost.localdomain name is often resolved via a DNS server (neither the OS nor the web browser is responsible for ensuring that localhost.localdomain is 127.0.0.1).
CVE-2017-18198	print_iso9660_recurse in iso-info.c in GNU libcdio before 1.0.0 allows remote attackers to cause a denial of service (heap-based buffer over-read) or possibly have unspecified other impact via a crafted iso file.
CVE-2017-18199	realloc_symlink in rock.c in GNU libcdio before 1.0.0 allows remote attackers to cause a denial of service (NULL Pointer Dereference) via a crafted iso file.
CVE-2017-18201	An issue was discovered in GNU libcdio before 2.0.0. There is a double free in get_cdtext_generic() in lib/driver/_cdio_generic.c.
CVE-2017-18205	In builtin.c in zsh before 5.4, when sh compatibility mode is used, there is a NULL pointer dereference during processing of the cd command with no argument if HOME is not set.
CVE-2017-18206	In utils.c in zsh before 5.4, symlink expansion had a buffer overflow.
CVE-2017-18232	The Serial Attached SCSI (SAS) implementation in the Linux kernel through 4.15.9 mishandles a mutex within libsas, which allows local users to cause a denial of service (deadlock) by triggering certain error-handling code.
CVE-2017-18233	An issue was discovered in Exempi before 2.4.4. Integer overflow in the Chunk class in XMPFiles/source/FormatSupport/RIFF.cpp allows remote attackers to cause a denial of service (infinite loop) via crafted XMP data in a .avi file.
CVE-2017-18234	An issue was discovered in Exempi before 2.4.3. It allows remote attackers to cause a denial of service (invalid memcpy with resultant use-after-free) or possibly have unspecified other impact via a .pdf file containing JPEG data, related to XMPFiles/source/FormatSupport/ReconcileTIFF.cpp, XMPFiles/source/FormatSupport/TIFF_MemoryReader.cpp, and XMPFiles/source/FormatSupport/TIFF_Support.hpp.
CVE-2017-18236	An issue was discovered in Exempi before 2.4.4. The ASF_Support::ReadHeaderObject function in XMPFiles/source/FormatSupport/ASF_Support.cpp allows remote

	attackers to cause a denial of service (infinite loop) via a crafted .asf file.
CVE-2017-18238	An issue was discovered in Exempi before 2.4.4. The TradQT_Manager::ParseCachedBoxes function in XMPFiles/source/FormatSupport/QuickTime_Support.cpp allows remote attackers to cause a denial of service (infinite loop) via crafted XMP data in a .qt file.
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-2017-18267	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-2017-18269	An SSE2-optimized memmove implementation for i386 in sysdeps/i386/i686/multiarch/memcpy-sse2-unaligned.S in the GNU C Library (aka glibc or libc6) 2.21 through 2.27 does not correctly perform the overlapping memory check if the source memory range spans the middle of the address space, resulting in corrupt data being produced by the copy operation. This may disclose information to context-dependent attackers, or result in a denial of service, or, possibly, code execution.
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-2017-3144	A vulnerability stemming from failure to properly clean up closed OMAPI connections can lead to exhaustion of the pool of socket descriptors available to the DHCP server. Affects ISC DHCP 4.1.0 to 4.1-ESV-R15, 4.2.0 to 4.2.8, 4.3.0 to 4.3.6. Older versions may also be affected but are well beyond their end-of-life (EOL). Releases prior to 4.1.0 have not been tested.
CVE-2017-3145	BIND was improperly sequencing cleanup operations on upstream recursion fetch contexts, leading in some cases to a use-after-free error that can trigger an assertion failure and crash in named. Affects BIND 9.0.0 to 9.8.x, 9.9.0 to 9.9.11, 9.10.0 to 9.10.6, 9.11.0 to 9.11.2, 9.9.3-S1 to 9.9.11-S1, 9.10.5-S1 to 9.10.6-S1, 9.12.0a1 to 9.12.0rc1.
CVE-2017-3636	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.56 and earlier and 5.6.36 and earlier. Easily exploitable vulnerability allows

	low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).
CVE-2017-3641	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3651	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2017-3653	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2017-3735	While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.

CVE-2017-3736	<p>There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.</p>
CVE-2017-3737	<p>OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.</p>
CVE-2017-3738	<p>There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the</p>

	DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.
CVE-2017-5006	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled object owner relationships, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-5007	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled the sequence of events when closing a page, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-5008	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed attacker controlled JavaScript to be run during the invocation of a private script method, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-5009	WebRTC in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5010	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, resolved promises in an inappropriate context, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2017-5011	Google Chrome prior to 56.0.2924.76 for Windows insufficiently sanitized DevTools URLs, which allowed a remote attacker who convinced a user to install a malicious extension to read filesystem contents via a crafted HTML page.
CVE-2017-5012	A heap buffer overflow in V8 in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2017-5013	Google Chrome prior to 56.0.2924.76 for Linux incorrectly handled new tab page navigations in non-selected tabs, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-5014	Heap buffer overflow during image processing in Skia in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5015	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, incorrectly handled Unicode glyphs, which allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5016	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to prevent certain UI elements from being displayed by non-visible pages, which allowed a remote attacker to show certain UI elements on a page they don't control via a crafted HTML page.
CVE-2017-5017	Interactions with the OS in Google Chrome prior to 56.0.2924.76 for Mac insufficiently cleared video memory, which allowed a remote attacker to possibly extract image fragments on systems with GeForce 8600M graphics chips via a crafted HTML page.
CVE-2017-5018	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, had an insufficiently strict content security policy on the Chrome app launcher page, which allowed a remote attacker to inject scripts or HTML into a privileged page via a crafted HTML page.
CVE-2017-5019	A use after free in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5020	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to require a user gesture for powerful download operations, which allowed a remote attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted HTML page.
CVE-2017-5021	A use after free in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5022	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to properly enforce unsafe-inline content security policy,

	which allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2017-5023	Type confusion in Histogram in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, allowed a remote attacker to potentially exploit a near null dereference via a crafted HTML page.
CVE-2017-5024	FFmpeg in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2017-5025	FFmpeg in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to perform proper bounds checking, which allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2017-5026	Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, failed to prevent alerts from being displayed by swapped out frames, which allowed a remote attacker to show alerts on a page they don't control via a crafted HTML page.
CVE-2017-5027	Blink in Google Chrome prior to 56.0.2924.76 for Linux, Windows and Mac, and 56.0.2924.87 for Android, failed to properly enforce unsafe-inline content security policy, which allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2017-5029	The xsltAddTextString function in transform.c in libxslt 1.1.29, as used in Blink in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android, lacked a check for integer overflow during a size calculation, which allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2017-5030	Incorrect handling of complex species in V8 in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac and 57.0.2987.108 for Android allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2017-5031	A use after free in ANGLE in Google Chrome prior to 57.0.2987.98 for Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5032	PDFium in Google Chrome prior to 57.0.2987.98 for Windows could be made to increment off the end of a buffer, which allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-5033	Blink in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android

	failed to correctly propagate CSP restrictions to local scheme pages, which allowed a remote attacker to bypass content security policy via a crafted HTML page, related to the unsafe-inline keyword.
CVE-2017-5034	A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Linux and Windows allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2017-5035	Google Chrome prior to 57.0.2987.98 for Windows and Mac had a race condition, which could cause Chrome to display incorrect certificate information for a site.
CVE-2017-5036	A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to have an unspecified impact via a crafted PDF file.
CVE-2017-5037	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5038	Chrome Apps in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac had a use after free bug in GuestView, which allowed a remote attacker to perform an out of bounds memory read via a crafted Chrome extension.
CVE-2017-5039	A use after free in PDFium in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-5040	V8 in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android was missing a neutering check, which allowed a remote attacker to read values in memory via a crafted HTML page.
CVE-2017-5041	Google Chrome prior to 57.0.2987.100 incorrectly handled back-forward navigation, which allowed a remote attacker to display incorrect information for a site via a crafted HTML page.
CVE-2017-5042	Cast in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android sent cookies to sites discovered via SSDP, which allowed an attacker on the local network segment to initiate connections to arbitrary URLs and observe any plaintext cookies sent.
CVE-2017-5043	Chrome Apps in Google Chrome prior to 57.0.2987.98 for Linux, Windows, and Mac had a use after free bug in GuestView, which allowed a remote attacker to perform an out of bounds memory read via a crafted Chrome extension.

CVE-2017-5044	Heap buffer overflow in filter processing in Skia in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5045	XSS Auditor in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed detection of a blocked iframe load, which allowed a remote attacker to brute force JavaScript variables via a crafted HTML page.
CVE-2017-5046	V8 in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android had insufficient policy enforcement, which allowed a remote attacker to spoof the location object via a crafted HTML page, related to Blink information disclosure.
CVE-2017-5047	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5048	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5049	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5050	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5051	An integer overflow in FFmpeg in Google Chrome prior to 57.0.2987.98 for Mac, Windows, and Linux and 57.0.2987.108 for Android allowed a remote attacker to perform an out of bounds memory write via a crafted video file, related to ChunkDemuxer.
CVE-2017-5052	An incorrect assumption about block structure in Blink in Google Chrome prior to 57.0.2987.133 for Mac, Windows, and Linux, and 57.0.2987.132 for Android, allowed a remote attacker to potentially exploit memory corruption via a crafted HTML page that triggers improper casting.
CVE-2017-5053	An out-of-bounds read in V8 in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker

	to execute arbitrary code inside a sandbox via a crafted HTML page, related to Array.prototype.indexOf.
CVE-2017-5054	An out-of-bounds read in V8 in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker to obtain heap memory contents via a crafted HTML page.
CVE-2017-5055	A use after free in printing in Google Chrome prior to 57.0.2987.133 for Linux and Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5056	A use after free in Blink in Google Chrome prior to 57.0.2987.133 for Linux, Windows, and Mac, and 57.0.2987.132 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5057	Type confusion in PDFium in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2017-5058	A use after free in PrintPreview in Google Chrome prior to 58.0.3029.81 for Windows allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2017-5059	Type confusion in Blink in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac, and 58.0.3029.83 for Android, allowed a remote attacker to potentially obtain code execution via a crafted HTML page.
CVE-2017-5060	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5061	A race condition in navigation in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-5062	A use after free in Chrome Apps in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to potentially perform out of bounds memory access via a crafted Chrome extension.
CVE-2017-5063	A numeric overflow in Skia in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac, and 58.0.3029.83 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.

CVE-2017-5064	Incorrect handling of DOM changes in Blink in Google Chrome prior to 58.0.3029.81 for Windows allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5065	Lack of an appropriate action on page navigation in Blink in Google Chrome prior to 58.0.3029.81 for Windows and Mac allowed a remote attacker to potentially confuse a user into making an incorrect security decision via a crafted HTML page.
CVE-2017-5066	Insufficient consistency checks in signature handling in the networking stack in Google Chrome prior to 58.0.3029.81 for Mac, Windows, and Linux, and 58.0.3029.83 for Android, allowed a remote attacker to incorrectly accept a badly formed X.509 certificate via a crafted HTML page.
CVE-2017-5067	An insufficient watchdog timer in navigation in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2017-5068	Incorrect handling of picture ID in WebRTC in Google Chrome prior to 58.0.3029.96 for Mac, Windows, and Linux allowed a remote attacker to trigger a race condition via a crafted HTML page.
CVE-2017-5069	Incorrect MIME type of XSS-Protection reports in Blink in Google Chrome prior to 58.0.3029.81 for Linux, Windows, and Mac, and 58.0.3029.83 for Android, allowed a remote attacker to circumvent Cross-Origin Resource Sharing checks via a crafted HTML page.
CVE-2017-5070	Type confusion in V8 in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2017-5071	Insufficient validation of untrusted input in V8 in Google Chrome prior to 59.0.3071.86 for Linux, Windows and Mac, and 59.0.3071.92 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5072	Inappropriate implementation in Omnibox in Google Chrome prior to 59.0.3071.92 for Android allowed a remote attacker to perform domain spoofing with RTL characters via a crafted URL page.
CVE-2017-5073	Use after free in print preview in Blink in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5074	A use after free in Chrome Apps in Google Chrome prior to 59.0.3071.86 for Windows allowed a remote

	attacker to perform an out of bounds memory read via a crafted HTML page, related to Bluetooth.
CVE-2017-5075	Inappropriate implementation in CSP reporting in Blink in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to obtain the value of url fragments via a crafted HTML page.
CVE-2017-5076	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5077	Insufficient validation of untrusted input in Skia in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac, and 59.0.3071.92 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5078	Insufficient validation of untrusted input in Blink's mailto: handling in Google Chrome prior to 59.0.3071.86 for Linux, Windows, and Mac allowed a remote attacker to perform command injection via a crafted HTML page, a similar issue to CVE-2004-0121. For example, characters such as * have an incorrect interaction with xdg-email in xdg-utils, and a space character can be used in front of a command-line argument.
CVE-2017-5079	Inappropriate implementation in Blink in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed a remote attacker to display UI on a non attacker controlled tab via a crafted HTML page.
CVE-2017-5080	A use after free in credit card autofill in Google Chrome prior to 59.0.3071.86 for Linux and Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5081	Lack of verification of an extension's locale folder in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed an attacker with local write access to modify extensions by modifying extension files.
CVE-2017-5082	Failure to take advantage of available mitigations in credit card autofill in Google Chrome prior to 59.0.3071.92 for Android allowed a local attacker to take screen shots of credit card information via a crafted HTML page.
CVE-2017-5083	Inappropriate implementation in Blink in Google Chrome prior to 59.0.3071.86 for Mac, Windows, and Linux, and 59.0.3071.92 for Android, allowed a remote attacker to display UI on a non attacker controlled tab via a crafted HTML page.

CVE-2017-5085	Inappropriate implementation in Bookmarks in Google Chrome prior to 59 for iOS allowed a remote attacker who convinced the user to perform certain operations to run JavaScript on chrome:// pages via a crafted bookmark.
CVE-2017-5086	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 59.0.3071.86 for Windows and Mac allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5087	A use after free in Blink in Google Chrome prior to 59.0.3071.104 for Mac, Windows, and Linux, and 59.0.3071.117 for Android, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page, aka an IndexedDB sandbox escape.
CVE-2017-5088	Insufficient validation of untrusted input in V8 in Google Chrome prior to 59.0.3071.104 for Mac, Windows, and Linux, and 59.0.3071.117 for Android, allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.
CVE-2017-5089	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 59.0.3071.104 for Mac allowed a remote attacker to perform domain spoofing via a crafted domain name.
CVE-2017-5091	A use after free in IndexedDB in Google Chrome prior to 60.0.3112.78 for Linux, Android, Windows, and Mac allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5092	Insufficient validation of untrusted input in PPAPI Plugins in Google Chrome prior to 60.0.3112.78 for Windows allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2017-5093	Inappropriate implementation in modal dialog handling in Blink in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to prevent a full screen warning from being displayed via a crafted HTML page.
CVE-2017-5094	Type confusion in extensions JavaScript bindings in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to potentially maliciously modify objects via a crafted HTML page.
CVE-2017-5095	Stack overflow in PDFium in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to potentially exploit stack corruption via a crafted PDF file.
CVE-2017-5097	Insufficient validation of untrusted input in Skia in Google Chrome prior to 60.0.3112.78 for Linux allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.

CVE-2017-5098	A use after free in V8 in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5099	Insufficient validation of untrusted input in PPAPI Plugins in Google Chrome prior to 60.0.3112.78 for Mac allowed a remote attacker to potentially gain privilege elevation via a crafted HTML page.
CVE-2017-5100	A use after free in Apps in Google Chrome prior to 60.0.3112.78 for Windows allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5101	Inappropriate implementation in Omnibox in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to spoof the contents of the Omnibox via a crafted HTML page.
CVE-2017-5102	Use of an uninitialized value in Skia in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5103	Use of an uninitialized value in Skia in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5104	Inappropriate implementation in interstitials in Google Chrome prior to 60.0.3112.78 for Mac allowed a remote attacker to spoof the contents of the omnibox via a crafted HTML page.
CVE-2017-5105	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5106	Insufficient Policy Enforcement in Omnibox in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to perform domain spoofing via IDN homographs in a crafted domain name.
CVE-2017-5107	A timing attack in SVG rendering in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to extract pixel values from a cross-origin page being iframe'd via a crafted HTML page.
CVE-2017-5108	Type confusion in PDFium in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to potentially maliciously modify objects via a crafted PDF file.

CVE-2017-5109	Inappropriate implementation of unload handler handling in permission prompts in Google Chrome prior to 60.0.3112.78 for Linux, Windows, and Mac allowed a remote attacker to display UI on a non attacker controlled tab via a crafted HTML page.
CVE-2017-5110	Inappropriate implementation of the web payments API on blob: and data: schemes in Web Payments in Google Chrome prior to 60.0.3112.78 for Mac, Windows, Linux, and Android allowed a remote attacker to spoof the contents of the Omnibox via a crafted HTML page.
CVE-2017-5111	A use after free in PDFium in Google Chrome prior to 61.0.3163.79 for Linux, Windows, and Mac allowed a remote attacker to potentially exploit memory corruption via a crafted PDF file.
CVE-2017-5112	Heap buffer overflow in WebGL in Google Chrome prior to 61.0.3163.79 for Windows allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2017-5113	Math overflow in Skia in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5114	Inappropriate use of partition alloc in PDFium in Google Chrome prior to 61.0.3163.79 for Linux, Windows, and Mac, and 61.0.3163.81 for Android, allowed a remote attacker to potentially exploit memory corruption via a crafted PDF file.
CVE-2017-5115	Type confusion in V8 in Google Chrome prior to 61.0.3163.79 for Windows allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2017-5116	Type confusion in V8 in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2017-5117	Use of an uninitialized value in Skia in Google Chrome prior to 61.0.3163.79 for Linux and Windows allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5118	Blink in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, failed to correctly propagate CSP restrictions to javascript scheme pages, which allowed a remote attacker to bypass content security policy via a crafted HTML page.

CVE-2017-5119	Use of an uninitialized value in Skia in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2017-5120	Inappropriate use of www mismatch redirects in browser navigation in Google Chrome prior to 61.0.3163.79 for Mac, Windows, and Linux, and 61.0.3163.81 for Android, allowed a remote attacker to potentially downgrade HTTPS requests to HTTP via a crafted HTML page. In other words, Chrome could transmit cleartext even though the user had entered an https URL, because of a misdesigned workaround for cases where the domain name in a URL almost matches the domain name in an X.509 server certificate (but differs in the initial "www." substring).
CVE-2017-5121	Inappropriate use of JIT optimisation in V8 in Google Chrome prior to 61.0.3163.100 for Linux, Windows, and Mac allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page, related to the escape analysis phase.
CVE-2017-5122	Inappropriate use of table size handling in V8 in Google Chrome prior to 61.0.3163.100 for Windows allowed a remote attacker to trigger out-of-bounds access via a crafted HTML page.
CVE-2017-5124	Incorrect application of sandboxing in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted MHTML page.
CVE-2017-5125	Heap buffer overflow in Skia in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-5126	A use after free in PDFium in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-5127	Use after free in PDFium in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2017-5128	Heap buffer overflow in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, related to WebGL.
CVE-2017-5129	A use after free in WebAudio in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2017-5130	An integer overflow in xmlmemory.c in libxml2 before 2.9.5, as used in Google Chrome prior to 62.0.3202.62

	and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted XML file.
CVE-2017-5131	An integer overflow in Skia in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka an out-of-bounds write.
CVE-2017-5132	Inappropriate implementation in V8 in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page, aka incorrect WebAssembly stack manipulation.
CVE-2017-5133	Off-by-one read/write on the heap in Blink in Google Chrome prior to 62.0.3202.62 allowed a remote attacker to corrupt memory and possibly leak information and potentially execute code via a crafted PDF file.
CVE-2017-5715	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-2017-5731	Bounds checking in Tianocompress before November 7, 2017 may allow an authenticated user to potentially enable an escalation of privilege via local access.
CVE-2017-5753	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
CVE-2017-5754	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 of the data cache.
CVE-2017-6059	Mod_auth_openidc.c in the Ping Identity OpenID Connect authentication module for Apache (aka mod_auth_openidc) before 2.14 allows remote attackers to spoof page content via a malicious URL provided to the user, which triggers an invalid request.
CVE-2017-6413	The "OpenID Connect Relying Party and OAuth 2.0 Resource Server" (aka mod_auth_openidc) module before 2.1.6 for the Apache HTTP Server does not skip OIDC_CLAIM_ and OIDCAuthNHeader headers in an "AuthType oauth20" configuration, which allows remote attackers to bypass authentication via crafted HTTP traffic.
CVE-2017-6462	Buffer overflow in the legacy Datum Programmable Time Server (DPTS) refclock driver in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows local users to have unspecified impact via a crafted /dev/datum device.
CVE-2017-6463	NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote authenticated users to cause a denial of service

	(daemon crash) via an invalid setting in a :config directive, related to the unpeer option.
CVE-2017-6464	NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote attackers to cause a denial of service (ntpd crash) via a malformed mode configuration directive.
CVE-2017-6519	avahi-daemon in Avahi through 0.6.32 and 0.7 inadvertently responds to IPv6 unicast queries with source addresses that are not on-link, which allows remote attackers to cause a denial of service (traffic amplification) and may cause information leakage by obtaining potentially sensitive information from the responding device via port-5353 UDP packets. NOTE: this may overlap CVE-2015-2809.
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-2017-7562	An authentication bypass flaw was found in the way krb5's certauth interface before 1.16.1 handled the validation of client certificates. A remote attacker able to communicate with the KDC could potentially use this flaw to impersonate arbitrary principals under rare and erroneous circumstances.
CVE-2017-8816	The NTLM authentication feature in curl and libcurl before 7.57.0 on 32-bit platforms allows attackers to cause a denial of service (integer overflow and resultant buffer overflow, and application crash) or possibly have unspecified other impact via vectors involving long user and password fields.
CVE-2017-8817	The FTP wildcard function in curl and libcurl before 7.57.0 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) or possibly have unspecified other impact via a string that ends with an '[' character.
CVE-2017-8818	curl and libcurl before 7.57.0 on 32-bit platforms allow attackers to cause a denial of service (out-of-bounds access and application crash) or possibly have unspecified other impact because too little memory is allocated for interfacing to an SSL library.
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-2018-0500	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-2018-0618	Cross-site scripting vulnerability in Mailman 2.1.26 and earlier allows remote authenticated attackers to inject arbitrary web script or HTML via unspecified vectors.
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-2018-0734	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).
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-2018-0739	Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).
CVE-2018-1000005	libcurl 7.49.0 to and including 7.57.0 contains an out bounds read in code handling HTTP/2 trailers. It was

	<p>reported (https://github.com/curl/curl/pull/2231) that reading an HTTP/2 trailer could mess up future trailers since the stored size was one byte less than required. The problem is that the code that creates HTTP/1-like headers from the HTTP/2 trailer data once appended a string like `:` to the target buffer, while this was recently changed to `: ` (a space was added after the colon) but the following math wasn't updated correspondingly. When accessed, the data is read out of bounds and causes either a crash or that the (too large) data gets passed to client write. This could lead to a denial-of-service situation or an information disclosure if someone has a service that echoes back or uses the trailers for something.</p>
CVE-2018-1000007	libcurl 7.1 through 7.57.0 might accidentally leak authentication data to third parties. When asked to send custom headers in its HTTP requests, libcurl will send that set of headers first to the host in the initial URL but also, if asked to follow redirects and a 30X HTTP response code is returned, to the host mentioned in URL in the `Location:` response header value. Sending the same set of headers to subsequent hosts is in particular a problem for applications that pass on custom `Authorization:` headers, as this header often contains privacy sensitive information or data that could allow others to impersonate the libcurl-using client's request.
CVE-2018-1000028	Linux kernel version after commit bdcf0a423ea1 - 4.15-rc4+, 4.14.8+, 4.9.76+, 4.4.111+ contains a Incorrect Access Control vulnerability in NFS server (nfsd) that can result in remote users reading or writing files they should not be able to via NFS. This attack appear to be exploitable via NFS server must export a filesystem with the "rootsquash" options enabled. This vulnerability appears to have been fixed in after commit 1995266727fa.
CVE-2018-1000035	A heap-based buffer overflow exists in Info-Zip UnZip version <= 6.00 in the processing of password-protected archives that allows an attacker to perform a denial of service or to possibly achieve code execution.
CVE-2018-1000073	RubyGems version Ruby 2.2 series: 2.2.9 and earlier, Ruby 2.3 series: 2.3.6 and earlier, Ruby 2.4 series: 2.4.3 and earlier, Ruby 2.5 series: 2.5.0 and earlier, prior to trunk revision 62422 contains a Directory Traversal vulnerability in install_location function of package.rb that can result in path traversal when writing to a symlinked basedir outside of the root. This vulnerability appears to have been fixed in 2.7.6.
CVE-2018-1000074	RubyGems version Ruby 2.2 series: 2.2.9 and earlier, Ruby 2.3 series: 2.3.6 and earlier, Ruby 2.4 series: 2.4.3 and earlier, Ruby 2.5 series: 2.5.0 and earlier,

	prior to trunk revision 62422 contains a Deserialization of Untrusted Data vulnerability in owner command that can result in code execution. This attack appear to be exploitable via victim must run the `gem owner` command on a gem with a specially crafted YAML file. This vulnerability appears to have been fixed in 2.7.6.
CVE-2018-1000075	RubyGems version Ruby 2.2 series: 2.2.9 and earlier, Ruby 2.3 series: 2.3.6 and earlier, Ruby 2.4 series: 2.4.3 and earlier, Ruby 2.5 series: 2.5.0 and earlier, prior to trunk revision 62422 contains a infinite loop caused by negative size vulnerability in ruby gem package tar header that can result in a negative size could cause an infinite loop.. This vulnerability appears to have been fixed in 2.7.6.
CVE-2018-1000076	RubyGems version Ruby 2.2 series: 2.2.9 and earlier, Ruby 2.3 series: 2.3.6 and earlier, Ruby 2.4 series: 2.4.3 and earlier, Ruby 2.5 series: 2.5.0 and earlier, prior to trunk revision 62422 contains a Improper Verification of Cryptographic Signature vulnerability in package.rb that can result in a mis-signed gem could be installed, as the tarball would contain multiple gem signatures.. This vulnerability appears to have been fixed in 2.7.6.
CVE-2018-1000077	RubyGems version Ruby 2.2 series: 2.2.9 and earlier, Ruby 2.3 series: 2.3.6 and earlier, Ruby 2.4 series: 2.4.3 and earlier, Ruby 2.5 series: 2.5.0 and earlier, prior to trunk revision 62422 contains a Improper Input Validation vulnerability in ruby gems specification homepage attribute that can result in a malicious gem could set an invalid homepage URL. This vulnerability appears to have been fixed in 2.7.6.
CVE-2018-1000078	RubyGems version Ruby 2.2 series: 2.2.9 and earlier, Ruby 2.3 series: 2.3.6 and earlier, Ruby 2.4 series: 2.4.3 and earlier, Ruby 2.5 series: 2.5.0 and earlier, prior to trunk revision 62422 contains a Cross Site Scripting (XSS) vulnerability in gem server display of homepage attribute that can result in XSS. This attack appear to be exploitable via the victim must browse to a malicious gem on a vulnerable gem server. This vulnerability appears to have been fixed in 2.7.6.
CVE-2018-1000079	RubyGems version Ruby 2.2 series: 2.2.9 and earlier, Ruby 2.3 series: 2.3.6 and earlier, Ruby 2.4 series: 2.4.3 and earlier, Ruby 2.5 series: 2.5.0 and earlier, prior to trunk revision 62422 contains a Directory Traversal vulnerability in gem installation that can result in the gem could write to arbitrary filesystem locations during installation. This attack appear to be exploitable via the victim must install a malicious gem. This vulnerability appears to have been fixed in 2.7.6.
CVE-2018-1000115	Memcached version 1.5.5 contains an Insufficient Control of Network Message Volume (Network

	Amplification, CWE-406) vulnerability in the UDP support of the memcached server that can result in denial of service via network flood (traffic amplification of 1:50,000 has been reported by reliable sources). This attack appear to be exploitable via network connectivity to port 11211 UDP. This vulnerability appears to have been fixed in 1.5.6 due to the disabling of the UDP protocol by default.
CVE-2018-1000119	Sinatra rack-protection versions 1.5.4 and 2.0.0.rc3 and earlier contains a timing attack vulnerability in the CSRF token checking that can result in signatures can be exposed. This attack appear to be exploitable via network connectivity to the ruby application. This vulnerability appears to have been fixed in 1.5.5 and 2.0.0.
CVE-2018-1000120	A buffer overflow exists in curl 7.12.3 to and including curl 7.58.0 in the FTP URL handling that allows an attacker to cause a denial of service or worse.
CVE-2018-1000121	A NULL pointer dereference exists in curl 7.21.0 to and including curl 7.58.0 in the LDAP code that allows an attacker to cause a denial of service
CVE-2018-1000122	A buffer over-read exists in curl 7.20.0 to and including curl 7.58.0 in the RTSP+RTP handling code that allows an attacker to cause a denial of service or information leakage
CVE-2018-1000140	rsyslog librelp version 1.2.14 and earlier contains a Buffer Overflow vulnerability in the checking of x509 certificates from a peer that can result in Remote code execution. This attack appear to be exploitable a remote attacker that can connect to rsyslog and trigger a stack buffer overflow by sending a specially crafted x509 certificate.
CVE-2018-1000156	GNU Patch version 2.7.6 contains an input validation vulnerability when processing patch files, specifically the EDITOR_PROGRAM invocation (using ed) can result in code execution. This attack appear to be exploitable via a patch file processed via the patch utility. This is similar to FreeBSD's CVE-2015-1418 however although they share a common ancestry the code bases have diverged over time.
CVE-2018-1000168	nghhttp2 version >= 1.10.0 and nghhttp2 <= v1.31.0 contains an Improper Input Validation CWE-20 vulnerability in ALTSVC frame handling that can result in segmentation fault leading to denial of service. This attack appears to be exploitable via network client. This vulnerability appears to have been fixed in >= 1.31.1.
CVE-2018-1000199	The Linux Kernel version 3.18 contains a dangerous feature vulnerability in modify_user_hw_breakpoint() that can result in crash and possibly memory corruption. This attack appear to be exploitable via

	local code execution and the ability to use ptrace. This vulnerability appears to have been fixed in git commit f67b15037a7a50c57f72e69a6d59941ad90a0f0f.
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-2018-1000852	FreeRDP FreeRDP 2.0.0-rc3 released version before commit 205c612820dac644d665b5bb1cdf437dc5ca01e3 contains a Other/Unknown vulnerability in channels/drdynvc/client/drdynvc_main.c, drdynvc_process_capability_request that can result in The RDP server can read the client's memory.. This attack appear to be exploitable via RDPClient must connect the rdp server with echo option. This vulnerability appears to have been fixed in after commit 205c612820dac644d665b5bb1cdf437dc5ca01e3.
CVE-2018-1000861	A code execution vulnerability exists in the Stapler web framework used by Jenkins 2.153 and earlier, LTS 2.138.3 and earlier in stapler/core/src/main/java/org/kohsuke/stapler/MetaClass.java that allows attackers to invoke some methods on Java objects by accessing crafted URLs that were not intended to be invoked this way.
CVE-2018-1000876	binutils version 2.32 and earlier contains a Integer Overflow vulnerability in objdump, bfd_get_dynamic_reloc_upper_bound,bfd_canonicalize_dynamic_reloc that can result in Integer overflow trigger heap overflow. Successful exploitation allows execution of arbitrary code.. This attack appear to be exploitable via Local. This vulnerability appears to have been fixed in after commit 3a551c7a1b80fca579461774860574eabfd7f18f.
CVE-2018-1000877	libarchive version commit 416694915449219d505531b1096384f3237dd6cc onwards (release v3.1.0 onwards) contains a CWE-415: Double Free vulnerability in RAR decoder - libarchive/archive_read_support_format_rar.c, parse_codes(), realloc(rar->lzss.window, new_size) with new_size = 0 that can result in Crash/DoS. This attack appear to be

	exploitable via the victim must open a specially crafted RAR archive.
CVE-2018-1000878	libarchive version commit 416694915449219d505531b1096384f3237dd6cc onwards (release v3.1.0 onwards) contains a CWE-416: Use After Free vulnerability in RAR decoder - libarchive/archive_read_support_format_rar.c that can result in Crash/DoS - it is unknown if RCE is possible. This attack appear to be exploitable via the victim must open a specially crafted RAR archive.
CVE-2018-1000888	PEAR Archive_Tar version 1.4.3 and earlier contains a CWE-502, CWE-915 vulnerability in the Archive_Tar class. There are several file operations with `'\$v_header['filename']` as parameter (such as file_exists, is_file, is_dir, etc). When extract is called without a specific prefix path, we can trigger unserialization by crafting a tar file with `phar:// [path_to_malicious_phar_file]` as path. Object injection can be used to trigger destruct in the loaded PHP classes, e.g. the Archive_Tar class itself. With Archive_Tar object injection, arbitrary file deletion can occur because `@unlink(\$this->_temp_tarname)` is called. If another class with useful gadget is loaded, it may possible to cause remote code execution that can result in files being deleted or possibly modified. This vulnerability appears to have been fixed in 1.4.4.
CVE-2018-1002105	In all Kubernetes versions prior to v1.10.11, v1.11.5, and v1.12.3, incorrect handling of error responses to proxied upgrade requests in the kube-apiserver allowed specially crafted requests to establish a connection through the Kubernetes API server to backend servers, then send arbitrary requests over the same connection directly to the backend, authenticated with the Kubernetes API server's TLS credentials used to establish the backend connection.
CVE-2018-1002200	plexus-archiver before 3.6.0 is vulnerable to directory traversal, allowing attackers to write to arbitrary files via a .. (dot dot slash) in an archive entry that is mishandled during extraction. This vulnerability is also known as 'Zip-Slip'.
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-2018-10323	The <code>xfs_bmap_extents_to_btree</code> function in <code>fs/xfs/libxfs/xfs_bmap.c</code> in the Linux kernel through 4.16.3 allows local users to cause a denial of service (<code>xfs_bmap_write</code> NULL pointer dereference) via a crafted <code>xfs</code> image.
CVE-2018-10360	The <code>do_core_note</code> function in <code>readelf.c</code> in <code>libmagic.a</code> 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-2018-10372	<code>process_cu_tu_index</code> in <code>dwarf.c</code> in GNU Binutils 2.30 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted binary file, as demonstrated by <code>readelf</code> .
CVE-2018-10373	<code>concat_filename</code> in <code>dwarf2.c</code> in the Binary File Descriptor (BFD) library (aka <code>libbfd</code>), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted binary file, as demonstrated by <code>nm-new</code> .
CVE-2018-1049	In systemd prior to 234 a race condition exists between <code>.mount</code> and <code>.automount</code> units such that automount requests from kernel may not be serviced by systemd resulting in kernel holding the mountpoint and any processes that try to use said mount will hang. A race condition like this may lead to denial of service, until mount points are unmounted.
CVE-2018-1050	All versions of Samba from 4.0.0 onwards are vulnerable to a denial of service attack when the RPC spoolss service is configured to be run as an external daemon. Missing input sanitization checks on some of the input parameters to spoolss RPC calls could cause the print spooler service to crash.
CVE-2018-10535	The <code>ignore_section_sym</code> function in <code>elf.c</code> in the Binary File Descriptor (BFD) library (aka <code>libbfd</code>), as distributed in GNU Binutils 2.30, does not validate the <code>output_section</code> pointer in the case of a <code>symsymtab</code> entry with a "SECTION" type that has a "0" value, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file, as demonstrated by <code>objcopy</code> .
CVE-2018-1054	An out-of-bounds memory read flaw was found in the way 389-ds-base handled certain LDAP search filters, affecting all versions including 1.4.x. A remote, unauthenticated attacker could potentially use this flaw to make ns-slapd crash via a specially crafted LDAP request, thus resulting in denial of service.
CVE-2018-1060	<code>python</code> before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking in <code>pop3lib</code> 's <code>apop()</code> method. An attacker could use this flaw to cause denial of service.

CVE-2018-1061	python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking in the difflib.IS_LINE_JUNK method. An attacker could use this flaw to cause denial of service.
CVE-2018-1063	Context relabeling of filesystems is vulnerable to symbolic link attack, allowing a local, unprivileged malicious entity to change the SELinux context of an arbitrary file to a context with few restrictions. This only happens when the relabeling process is done, usually when taking SELinux state from disabled to enable (permissive or enforcing). The issue was found in policycoreutils 2.5-11.
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-2018-10675	The do_get_mempolicy function in mm/mempolicy.c in the Linux kernel before 4.12.9 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted system calls.
CVE-2018-1068	A flaw was found in the Linux 4.x kernel's implementation of 32-bit syscall interface for bridging. This allowed a privileged user to arbitrarily write to a limited range of kernel memory.
CVE-2018-10689	blktrace (aka Block IO Tracing) 1.2.0, as used with the Linux kernel and Android, has a buffer overflow in the dev_map_read function in btt/devmap.c because the device and devno arrays are too small, as demonstrated by an invalid free when using the btt program with a crafted file.
CVE-2018-1071	zsh through version 5.4.2 is vulnerable to a stack-based buffer overflow in the exec.c:hashcmd() function. A local attacker could exploit this to cause a denial of service.
CVE-2018-10754	A NULL pointer dereference was found in the way the _nc_parse_entry function parses terminfo data for compilation. An attacker able to provide specially crafted terminfo data could use this flaw to crash the application parsing it.
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-2018-10772	The tExToDataBuf function in pngimage.cpp in Exiv2 through 0.26 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file.

CVE-2018-10779	TIFFWriteScanline in tif_write.c in LibTIFF 3.8.2 has a heap-based buffer over-read, as demonstrated by bmp2tiff.
CVE-2018-1079	pcsd before version 0.9.164 and 0.10 is vulnerable to a privilege escalation via authorized user malicious REST call. The REST interface of the pcasd service did not properly sanitize the file name from the /remote/put_file query. If the /etc/booth directory exists, an authenticated attacker with write permissions could create or overwrite arbitrary files with arbitrary data outside of the /etc/booth directory, in the context of the pcasd process.
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-2018-1083	Zsh before version 5.4.2-test-1 is vulnerable to a buffer overflow in the shell autocomplete functionality. A local unprivileged user can create a specially crafted directory path which leads to code execution in the context of the user who tries to use autocomplete to traverse the before mentioned path. If the user affected is privileged, this leads to privilege escalation.
CVE-2018-1084	corosync before version 2.4.4 is vulnerable to an integer overflow in exec/totemcrypto.c.
CVE-2018-10844	It was found that the GnuTLS implementation of HMAC-SHA-256 was vulnerable to a Lucky thirteen style attack. Remote attackers could use this flaw to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data using crafted packets.
CVE-2018-10845	It was found that the GnuTLS implementation of HMAC-SHA-384 was vulnerable to a Lucky thirteen style attack. Remote attackers could use this flaw to conduct distinguishing attacks and plain text recovery attacks via statistical analysis of timing data using crafted packets.
CVE-2018-10846	A cache-based side channel in GnuTLS implementation that leads to plain text recovery in cross-VM attack setting was found. An attacker could use a combination of "Just in Time" Prime+probe attack in combination with Lucky-13 attack to recover plain text using crafted packets.
CVE-2018-10850	389-ds-base before versions 1.4.0.10, 1.3.8.3 is vulnerable to a race condition in the way 389-ds-base handles persistent search, resulting in a crash if the server is under load. An anonymous attacker could use this flaw to trigger a denial of service.
CVE-2018-10852	The UNIX pipe which sudo uses to contact SSSD and read the available sudo rules from SSSD has too wide

	permissions, which means that anyone who can send a message using the same raw protocol that sudo and SSSD use can read the sudo rules available for any user. This affects versions of SSSD before 1.16.3.
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-2018-1086	pcs before versions 0.9.164 and 0.10 is vulnerable to a debug parameter removal bypass. REST interface of the pcsd service did not properly remove the pcs debug argument from the /run_pcs query, possibly disclosing sensitive information. A remote attacker with a valid token could use this flaw to elevate their privilege.
CVE-2018-1087	kernel KVM before versions kernel 4.16, kernel 4.16-rc7, kernel 4.17-rc1, kernel 4.17-rc2 and kernel 4.17-rc3 is vulnerable to a flaw in the way the Linux kernel's KVM hypervisor handled exceptions delivered after a stack switch operation via Mov SS or Pop SS instructions. During the stack switch operation, the processor did not deliver interrupts and exceptions, rather they are delivered once the first instruction after the stack switch is executed. An unprivileged KVM guest user could use this flaw to crash the guest or, potentially, escalate their privileges in the guest.
CVE-2018-1089	389-ds-base before versions 1.4.0.9, 1.3.8.1, 1.3.6.15 did not properly handle long search filters with characters needing escapes, possibly leading to buffer overflows. A remote, unauthenticated attacker could potentially use this flaw to make ns-slapd crash via a specially crafted LDAP request, thus resulting in denial of service.
CVE-2018-10892	The default OCI linux spec in oci/defaults_{linux}.go in Docker/Moby from 1.11 to current does not block /proc/acpi pathnames. The flaw allows an attacker to modify host's hardware like enabling/disabling bluetooth or turning up/down keyboard brightness.
CVE-2018-10893	Multiple integer overflow and buffer overflow issues were discovered in spice-client's handling of LZ compressed frames. A malicious server could cause the client to crash or, potentially, execute arbitrary code.
CVE-2018-10896	The default cloud-init configuration, in cloud-init 0.6.2 and newer, included "ssh_deletekeys: 0", disabling cloud-init's deletion of ssh host keys. In some environments, this could lead to instances created by cloning a golden master or template system, sharing ssh host keys, and being able to impersonate one another or conduct man-in-the-middle attacks.

CVE-2018-10897	A directory traversal issue was found in reposync, a part of yum-utils, where reposync fails to sanitize paths in remote repository configuration files. If an attacker controls a repository, they may be able to copy files outside of the destination directory on the targeted system via path traversal. If reposync is running with heightened privileges on a targeted system, this flaw could potentially result in system compromise via the overwriting of critical system files. Version 1.1.31 and older are believed to be affected.
CVE-2018-10901	A flaw was found in Linux kernel's KVM virtualization subsystem. The VMX code does not restore the GDT.LIMIT to the previous host value, but instead sets it to 64KB. With a corrupted GDT limit a host's userspace code has an ability to place malicious entries in the GDT, particularly to the per-cpu variables. An attacker can use this to escalate their privileges.
CVE-2018-10906	In fuse before versions 2.9.8 and 3.x before 3.2.5, fusermount is vulnerable to a restriction bypass when SELinux is active. This allows non-root users to mount a FUSE file system with the 'allow_other' mount option regardless of whether 'user_allow_other' is set in the fuse configuration. An attacker may use this flaw to mount a FUSE file system, accessible by other users, and trick them into accessing files on that file system, possibly causing Denial of Service or other unspecified effects.
CVE-2018-1091	In the flush_tmregs_to_thread function in arch/powerpc/kernel/ptrace.c in the Linux kernel before 4.13.5, a guest kernel crash can be triggered from unprivileged userspace during a core dump on a POWER host due to a missing processor feature check and an erroneous use of transactional memory (TM) instructions in the core dump path, leading to a denial of service.
CVE-2018-10911	A flaw was found in the way dic_unserialize function of glusterfs does not handle negative key length values. An attacker could use this flaw to read memory from other locations into the stored dict value.
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-2018-10916	It has been discovered that lftp up to and including version 4.8.3 does not properly sanitize remote file

	names, leading to a loss of integrity on the local system when reverse mirroring is used. A remote attacker may trick a user to use reverse mirroring on an attacker controlled FTP server, resulting in the removal of all files in the current working directory of the victim's system.
CVE-2018-10932	lldptool version 1.0.1 and older can print a raw, unsanitized attacker controlled buffer when mngAddr information is displayed. This may allow an attacker to inject shell control characters into the buffer and impact the behavior of the terminal.
CVE-2018-10935	A flaw was found in the 389 Directory Server that allows users to cause a crash in the LDAP server using ldapsearch with server side sort.
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-2018-10963	The TIFFWriteDirectorySec() function in tif_dirwrite.c in LibTIFF through 4.0.9 allows remote attackers to cause a denial of service (assertion failure and application crash) via a crafted file, a different vulnerability than CVE-2017-13726.
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-2018-1100	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-2018-11037	In Exiv2 0.26, the Exiv2::PngImage::printStructure function in pngimage.cpp allows remote attackers to cause an information leak via a crafted file.
CVE-2018-1106	An authentication bypass flaw has been found in PackageKit before 1.1.10 that allows users without administrator privileges to install signed packages. A local attacker can use this vulnerability to install vulnerable packages to further compromise a system.
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-2018-1111	DHCP packages in Red Hat Enterprise Linux 6 and 7, Fedora 28, and earlier are vulnerable to a command injection flaw in the NetworkManager integration script included in the DHCP client. A malicious DHCP server, or an attacker on the local network able to spoof DHCP responses, could use this flaw to execute arbitrary

	commands with root privileges on systems using NetworkManager and configured to obtain network configuration using the DHCP protocol.
CVE-2018-1113	setup before version 2.11.4-1.fc28 in Fedora and Red Hat Enterprise Linux added /sbin/nologin and /usr/sbin/nologin to /etc/shells. This violates security assumptions made by pam_shells and some daemons which allow access based on a user's shell being listed in /etc/shells. Under some circumstances, users which had their shell changed to /sbin/nologin could still access the system.
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-2018-1120	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 and 9d. The alloc_sarray function in jmemmgr.c allows remote attackers to cause a denial of service (divide-by-zero error) via a crafted file.
CVE-2018-11213	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-2018-11233	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-2018-11236	stdlib/canonicalize.c in the GNU C Library (aka glibc or libc6) 2.27 and earlier, when processing very long pathname arguments to the realpath function, could encounter an integer overflow on 32-bit architectures, leading to a stack-based buffer overflow and, potentially, arbitrary code execution.
CVE-2018-11237	An AVX-512-optimized implementation of the mempcpy function in the GNU C Library (aka glibc or libc6) 2.27 and earlier may write data beyond the target buffer, leading to a buffer overflow in __mempcpy_avx512_no_vzeroupper.
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-2018-1126	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-2018-11362	In Wireshark 2.6.0, 2.4.0 to 2.4.6, and 2.2.0 to 2.2.14, the LDSS dissector could crash. This was addressed in epan/dissectors/packet-lrss.c by avoiding a buffer over-read upon encountering a missing '0' character.
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-2018-11412	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-2018-11439	The TagLib::Ogg::FLAC::File::scan function in oggflacfile.cpp in TagLib 1.11.1 allows remote attackers to cause information disclosure (heap-based buffer over-read) via a crafted audio file.
CVE-2018-11577	Liblouis 3.5.0 has a Segmentation fault in lou_logPrint in logging.c.
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-2018-11656	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-2018-11684	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-2018-1172	This vulnerability allows remote attackers to deny service on vulnerable installations of The Squid Software Foundation Squid 3.5.27-20180318. Authentication is not required to exploit this vulnerability. The specific flaw exists within ClientRequestContext::sslBumpAccessCheck(). A crafted request can trigger the dereference of a null pointer. An attacker can leverage this vulnerability to create a denial-of-service condition to users of the system. Was ZDI-CAN-6088.
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-2018-11769	CouchDB administrative users before 2.2.0 can configure the database server via HTTP(S). Due to insufficient validation of administrator-supplied configuration settings via the HTTP API, it is possible for a CouchDB administrator user to escalate their privileges to that of the operating system's user under which CouchDB runs, by bypassing the blacklist of configuration settings that are not allowed to be modified via the HTTP API. This privilege escalation effectively allows a CouchDB admin user to gain arbitrary remote code execution, bypassing CVE-2017-12636 and CVE-2018-8007.

CVE-2018-11781	Apache SpamAssassin 3.4.2 fixes a local user code injection in the meta rule syntax.
CVE-2018-11782	In Apache Subversion versions up to and including 1.9.10, 1.10.4, 1.12.0, Subversion's svnserve server process may exit when a well-formed read-only request produces a particular answer. This can lead to disruption for users of the server.
CVE-2018-11784	When the default servlet in Apache Tomcat versions 9.0.0.M1 to 9.0.11, 8.5.0 to 8.5.33 and 7.0.23 to 7.0.90 returned a redirect to a directory (e.g. redirecting to '/foo/' when the user requested '/foo') a specially crafted URL could be used to cause the redirect to be generated to any URI of the attackers choice.
CVE-2018-11806	m_cat in slirp/mbuf.c in Qemu has a heap-based buffer overflow via incoming fragmented datagrams.
CVE-2018-11813	libjpeg 9c has a large loop because read_pixel in rdtarga.c mishandles EOF.
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-2018-12121	Node.js: All versions prior to Node.js 6.15.0, 8.14.0, 10.14.0 and 11.3.0: Denial of Service with large HTTP headers: By using a combination of many requests with maximum sized headers (almost 80 KB per connection), and carefully timed completion of the headers, it is possible to cause the HTTP server to abort from heap allocation failure. Attack potential is mitigated by the use of a load balancer or other proxy layer.
CVE-2018-12126	Microarchitectural Store Buffer Data Sampling (MSBDS): Store buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/

	documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf
CVE-2018-12127	Microarchitectural Load Port Data Sampling (MLPDS): Load ports on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf
CVE-2018-12130	Microarchitectural Fill Buffer Data Sampling (MFBDS): Fill buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf
CVE-2018-12178	Buffer overflow in network stack for EDK II may allow unprivileged user to potentially enable escalation of privilege and/or denial of service via network.
CVE-2018-12179	Improper configuration in system firmware for EDK II may allow unauthenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via local access.
CVE-2018-12180	Buffer overflow in BlockIo service for EDK II may allow an unauthenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via network access.
CVE-2018-12181	Stack overflow in corrupted bmp for EDK II may allow unprivileged user to potentially enable denial of service or elevation of privilege via local access.
CVE-2018-12182	Insufficient memory write check in SMM service for EDK II may allow an authenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via local access.
CVE-2018-12183	Stack overflow in DxeCore for EDK II may allow an unauthenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via local access.
CVE-2018-12207	Improper invalidation for page table updates by a virtual guest operating system for multiple Intel(R) Processors may allow an authenticated user to potentially enable denial of service of the host system via local access.
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-2018-12264	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-2018-12327	Stack-based buffer overflow in ntpq and ntpdc of NTP version 4.2.8p11 allows an attacker to achieve code execution or escalate to higher privileges via a long string as the argument for an IPv4 or IPv6 command-line parameter. NOTE: It is unclear whether there are any common situations in which ntpq or ntpdc is used with a command line from an untrusted source.
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-2018-12362	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-2018-12372	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	Decrypted 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-2018-12384	When handling a SSLv2-compatible ClientHello request, the server doesn't generate a new random value but sends an all-zero value instead. This results in full malleability of the ClientHello for SSLv2 used for TLS 1.2 in all versions prior to NSS 3.39. This does not impact TLS 1.3.
CVE-2018-12389	Mozilla developers and community members reported memory safety bugs present in Firefox ESR 60.2. 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 ESR < 60.3 and Thunderbird < 60.3.
CVE-2018-12390	Mozilla developers and community members reported memory safety bugs present in Firefox 62 and Firefox ESR 60.2. 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 < 63, Firefox ESR < 60.3, and Thunderbird < 60.3.
CVE-2018-12392	When manipulating user events in nested loops while opening a document through script, it is possible to

	trigger a potentially exploitable crash due to poor event handling. This vulnerability affects Firefox < 63, Firefox ESR < 60.3, and Thunderbird < 60.3.
CVE-2018-12393	A potential vulnerability was found in 32-bit builds where an integer overflow during the conversion of scripts to an internal UTF-16 representation could result in allocating a buffer too small for the conversion. This leads to a possible out-of-bounds write. *Note: 64-bit builds are not vulnerable to this issue.*. This vulnerability affects Firefox < 63, Firefox ESR < 60.3, and Thunderbird < 60.3.
CVE-2018-12404	A cached side channel attack during handshakes using RSA encryption could allow for the decryption of encrypted content. This is a variant of the Adaptive Chosen Ciphertext attack (AKA Bleichenbacher attack) and affects all NSS versions prior to NSS 3.41.
CVE-2018-12405	Mozilla developers and community members reported memory safety bugs present in Firefox 63 and Firefox ESR 60.3. 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 Thunderbird < 60.4, Firefox ESR < 60.4, and Firefox < 64.
CVE-2018-12599	In ImageMagick 7.0.8-3 Q16, ReadBMPIImage and WriteBMPIImage 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-2018-12641	An issue was discovered in arm_pt in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. Stack Exhaustion occurs in the C++ demangling functions provided by libiberty, and there are recursive stack frames: demangle_arm_hp_template, demangle_class_name, demangle_fund_type, do_type, do_arg, demangle_args, and demangle_nested_args. This can occur during execution of nm-new.
CVE-2018-12697	A NULL pointer dereference (aka SEGV on unknown address 0x00000000000000) was discovered in work_stuff_copy_to_from in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. This can occur during execution of objdump.
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-2018-12900	Heap-based buffer overflow in the cpSeparateBufToContigBuf function in tiffcp.c in LibTIFF 3.9.3, 3.9.4, 3.9.5, 3.9.6, 3.9.7, 4.0.0beta7, 4.0.0alpha4, 4.0.0alpha5, 4.0.0alpha6, 4.0.0, 4.0.1, 4.0.2, 4.0.3, 4.0.4, 4.0.4beta, 4.0.5, 4.0.6, 4.0.7, 4.0.8 and 4.0.9 allows remote attackers to cause a denial of service (crash) or possibly have unspecified other impact via a crafted TIFF file.
CVE-2018-13033	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted ELF file, as demonstrated by _bfd_elf_parse_attributes in elf-attrs.c and bfd_malloc in libbfd.c. This can occur during execution of nm.
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-2018-1305	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-2018-13093	An issue was discovered in fs/xfs/xfs_icache.c in the Linux kernel through 4.17.3. There is a NULL pointer dereference and panic in lookup_slow() on a NULL inode->i_ops pointer when doing pathwalks on a corrupted xfs image. This occurs because of a lack of

	proper validation that cached inodes are free during allocation.
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-2018-1311	The Apache Xerces-C 3.0.0 to 3.2.3 XML parser contains a use-after-free error triggered during the scanning of external DTDs. This flaw has not been addressed in the maintained version of the library and has no current mitigation other than to disable DTD processing. This can be accomplished via the DOM using a standard parser feature, or via SAX using the XERCES_DISABLE_DTD environment variable.
CVE-2018-13139	A stack-based buffer overflow in psf_memset in common.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted audio file. The vulnerability can be triggered by the executable sndfile-deinterleave.
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-2018-1336	An improper handing of overflow in the UTF-8 decoder with supplementary characters can lead to an infinite loop in the decoder causing a Denial of Service. Versions Affected: Apache Tomcat 9.0.0.M9 to 9.0.7, 8.5.0 to 8.5.30, 8.0.0.RC1 to 8.0.51, and 7.0.28 to 7.0.86.
CVE-2018-13440	The audiofile Audio File Library 0.3.6 has a NULL pointer dereference bug in ModuleState::setup in modules/ModuleState.cpp, which allows an attacker to cause a denial of service via a crafted caf file, as demonstrated by sfconvert.
CVE-2018-13796	An issue was discovered in GNU Mailman before 2.1.28. A crafted URL can cause arbitrary text to be displayed on a web page from a trusted site.
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-2018-14040	In Bootstrap before 4.1.2, XSS is possible in the collapse data-parent attribute.

CVE-2018-14042	In Bootstrap before 4.1.2, XSS is possible in the data-container property of tooltip.
CVE-2018-14046	Exiv2 0.26 has a heap-based buffer over-read in WebPImage::decodeChunks in webpimage.cpp.
CVE-2018-14340	In Wireshark 2.6.0 to 2.6.1, 2.4.0 to 2.4.7, and 2.2.0 to 2.2.15, dissectors that support zlib decompression could crash. This was addressed in epan/tvbuff_zlib.c by rejecting negative lengths to avoid a buffer over-read.
CVE-2018-14341	In Wireshark 2.6.0 to 2.6.1, 2.4.0 to 2.4.7, and 2.2.0 to 2.2.15, the DICOM dissector could go into a large or infinite loop. This was addressed in epan/dissectors/packet-dcm.c by preventing an offset overflow.
CVE-2018-14348	libcgroup up to and including 0.41 creates /var/log/cgred with mode 0666 regardless of the configured umask, leading to disclosure of information.
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-2018-14357	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-2018-14362	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-2018-14368	In Wireshark 2.6.0 to 2.6.1, 2.4.0 to 2.4.7, and 2.2.0 to 2.2.15, the Bazaar protocol dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-bzr.c by properly handling items that are too long.
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-2018-14434	ImageMagick 7.0.8-4 has a memory leak for a colormap in WriteMPCLImage 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 ReadMIFImage in coders/miff.c.
CVE-2018-14437	ImageMagick 7.0.8-4 has a memory leak in parse8BIM in coders/meta.c.
CVE-2018-14498	get_8bit_row in rdbmp.c in libjpeg-turbo through 1.5.90 and MozJPEG through 3.3.1 allows attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted 8-bit BMP in which one or more of the color indices is out of range for the number of palette entries.
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-2018-14567	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-2018-14598	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-2018-14618	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.)
CVE-2018-14624	A vulnerability was discovered in 389-ds-base through versions 1.3.7.10, 1.3.8.8 and 1.4.0.16. The lock controlling the error log was not correctly used when re-opening the log file in log_error_emergency(). An attacker could send a flood of modifications to a very large DN, which would cause slapd to crash.
CVE-2018-14625	A flaw was found in the Linux Kernel where an attacker may be able to have an uncontrolled read to kernel-memory from within a vm guest. A race condition between connect() and close() function may allow an attacker using the AF_VSOCK protocol to gather a 4 byte information leak or possibly intercept or corrupt AF_VSOCK messages destined to other clients.
CVE-2018-14633	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.
CVE-2018-14634	An integer overflow flaw was found in the Linux kernel's create_elf_tables() function. An unprivileged local user with access to SUID (or otherwise privileged) binary could use this flaw to escalate their privileges on the system. Kernel versions 2.6.x, 3.10.x and 4.14.x are believed to be vulnerable.
CVE-2018-14638	A flaw was found in 389-ds-base before version 1.3.8.4-13. The process ns-slapd crashes in delete_passwdPolicy function when persistent search connections are terminated unexpectedly leading to remote 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. The vulnerability exists in Python versions 3.7.0, 3.6.0 through 3.6.6, 3.5.0 through 3.5.6, 3.4.0 through 3.4.9, 2.7.0 through 2.7.15.

CVE-2018-14648	A flaw was found in 389 Directory Server. A specially crafted search query could lead to excessive CPU consumption in the do_search() function. An unauthenticated attacker could use this flaw to provoke a denial of service.
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-2018-15127	LibVNC before commit 502821828ed00b4a2c4bef90683d0fd88ce495de contains heap out-of-bound write vulnerability in server code of file transfer extension that can result remote code execution
CVE-2018-15473	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.
CVE-2018-15518	QXmlStream in Qt 5.x before 5.11.3 has a double-free or corruption during parsing of a specially crafted illegal XML document.
CVE-2018-15587	GNOME Evolution through 3.28.2 is prone to OpenPGP signatures being spoofed for arbitrary messages using a specially crafted email that contains a valid signature from the entity to be impersonated as an attachment.
CVE-2018-15594	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.
CVE-2018-15607	In ImageMagick 7.0.8-11 Q16, a tiny input file 0x50 0x36 0x36 0x36 0x36 0x4c 0x36 0x38 0x36 0x36 0x36 0x36 0x36 0x36 0x36 0x1f 0x35 0x50 0x00 can result in a hang of several minutes during which CPU and memory resources are consumed until ultimately an attempted large memory allocation fails. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted file.

CVE-2018-15664	In Docker through 18.06.1-ce-rc2, the API endpoints behind the 'docker cp' command are vulnerable to a symlink-exchange attack with Directory Traversal, giving attackers arbitrary read-write access to the host filesystem with root privileges, because daemon/archive.go does not do archive operations on a frozen filesystem (or from within a chroot).
CVE-2018-15686	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.
CVE-2018-15688	A buffer overflow vulnerability in the dhcpc6 client of systemd allows a malicious dhcpc6 server to overwrite heap memory in systemd-networkd. Affected releases are systemd: versions up to and including 239.
CVE-2018-15715	Zoom clients on Windows (before version 4.1.34814.1119), Mac OS (before version 4.1.34801.1116), and Linux (2.4.129780.0915 and below) are vulnerable to unauthorized message processing. A remote unauthenticated attacker can spoof UDP messages from a meeting attendee or Zoom server in order to invoke functionality in the target client. This allows the attacker to remove attendees from meetings, spoof messages from users, or hijack shared screens.
CVE-2018-15853	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-2018-15859	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-2018-15982	Flash Player versions 31.0.0.153 and earlier, and 31.0.0.108 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2018-15983	Flash Player versions 31.0.0.153 and earlier, and 31.0.0.108 and earlier have an insecure library loading (dll hijacking) vulnerability. Successful exploitation could lead to privilege escalation.
CVE-2018-16057	In Wireshark 2.6.0 to 2.6.2, 2.4.0 to 2.4.8, and 2.2.0 to 2.2.16, the Radiotap dissector could crash. This was addressed in epan/dissectors/packet-ieee80211-radiotap-iter.c by validating iterator operations.
CVE-2018-16062	dwarf_getaranges in dwarf_getaranges.c in libdw in elfutils before 2018-08-18 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted file.
CVE-2018-16065	A Javascript reentrancy issues that caused a use-after-free in V8 in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-16066	A use after free in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-16067	A use after free in WebAudio in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-16068	Missing validation in Mojo in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2018-16069	Unintended floating-point error accumulation in SwiftShader in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-16070	Integer overflows in Skia in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-16071	A use after free in WebRTC in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2018-16073	Insufficient policy enforcement in site isolation in Google Chrome prior to 69.0.3497.81 allowed a remote

	attacker to bypass site isolation via a crafted HTML page.
CVE-2018-16074	Insufficient policy enforcement in site isolation in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2018-16075	Insufficient file type enforcement in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to obtain local file data via a crafted HTML page.
CVE-2018-16076	Missing bounds check in PDFium in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2018-16077	Object lifecycle issue in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2018-16078	Unsafe handling of credit card details in Autofill in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2018-16079	A race condition between permission prompts and navigations in Prompts in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-16080	A missing check for popup window handling in Fullscreen in Google Chrome on macOS prior to 69.0.3497.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-16081	Allowing the chrome.debugger API to run on file:// URLs in DevTools in Google Chrome prior to 69.0.3497.81 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system without file access permission via a crafted Chrome Extension.
CVE-2018-16082	An out of bounds read in Swiftshader in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2018-16083	An out of bounds read in forward error correction code in WebRTC in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-16084	The default selected dialog button in CustomHandlers in Google Chrome prior to 69.0.3497.81 allowed a remote attacker who convinced the user to perform certain operations to open external programs via a crafted HTML page.

CVE-2018-16085	A use after free in ResourceCoordinator in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-16328	In ImageMagick before 7.0.8-8, a NULL pointer dereference exists in the CheckEventLogging function in MagickCore/log.c.
CVE-2018-16391	Several buffer overflows when handling responses from a Muscle Card in muscle_list_files in libopencsc/card-muscle.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.
CVE-2018-16392	Several buffer overflows when handling responses from a TCOS Card in tcos_select_file in libopencsc/card-tcos.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.
CVE-2018-16393	Several buffer overflows when handling responses from a Gmsafe V1 Smartcard in gmsafe_get_cert_len in libopencsc/pkcs15-gmsafeV1.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.
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-2018-16402	libelf/elf_end.c in elfutils 0.173 allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact because it tries to decompress twice.
CVE-2018-16403	libdw in elfutils 0.173 checks the end of the attributes list incorrectly in dwarf_getabbrev in dwarf_getabbrev.c

	and dwarf_hasattr in dwarf_hasattr.c, leading to a heap-based buffer over-read and an application crash.
CVE-2018-16418	A buffer overflow when handling string concatenation in util_acl_to_str in tools/util.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.
CVE-2018-16419	Several buffer overflows when handling responses from a Cryptoflex card in read_public_key in tools/cryptoflex-tool.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.
CVE-2018-16420	Several buffer overflows when handling responses from an ePass 2003 Card in decrypt_response in libopencsc/card-epass2003.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.
CVE-2018-16421	Several buffer overflows when handling responses from a CAC Card in cac_get_serial_nr_from_CUID in libopencsc/card-cac.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.
CVE-2018-16422	A single byte buffer overflow when handling responses from an esteid Card in sc_pkcs15emu_esteem_init in libopencsc/pkcs15-esteid.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.
CVE-2018-16423	A double free when handling responses from a smartcard in sc_file_set_sec_attr in libopencsc/sc.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to cause a denial of service (application crash) or possibly have unspecified other impact.
CVE-2018-16426	Endless recursion when handling responses from an IAS-ECC card in iasecc_select_file in libopencsc/card-iasecc.c in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to hang or crash the opencsc library using programs.
CVE-2018-16427	Various out of bounds reads when handling responses in OpenSC before 0.19.0-rc1 could be used by attackers able to supply crafted smartcards to potentially crash the opencsc library using programs.
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-2018-16511	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-2018-16548	An issue was discovered in ZZIPlib through 0.13.69. There is a memory leak triggered in the function __zzip_parse_root_directory in zip.c, which will lead to a denial of service attack.
CVE-2018-16585	** DISPUTED ** 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. Note: A reputable source believes that the CVE is potentially a duplicate of CVE-2018-15910 as explained in Red Hat bugzilla (https://bugzilla.redhat.com/show_bug.cgi?id=1626193).
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-2018-16658	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.
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-2018-16838	A flaw was found in sssd Group Policy Objects implementation. When the GPO is not readable by SSSD due to a too strict permission settings on the server side, SSSD will allow all authenticated users to login instead of denying access.
CVE-2018-16839	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.
CVE-2018-16840	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.
CVE-2018-16842	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.
CVE-2018-1685	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 contains a vulnerability in db2cacpy that could allow a local user to read any file on the system. IBM X-Force ID: 145502.
CVE-2018-16862	A security flaw was found in the Linux kernel in a way that the cleancache subsystem clears an inode after the final file truncation (removal). The new file created with the same inode may contain leftover pages from cleancache and the old file data instead of the new one.
CVE-2018-16864	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when a program with long command line arguments calls syslog. A local

	attacker may use this flaw to crash systemd-journald or escalate his privileges. Versions through v240 are vulnerable.
CVE-2018-16865	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when many entries are sent to the journal socket. A local attacker, or a remote one if systemd-journal-remote is used, may use this flaw to crash systemd-journald or execute code with journald privileges. Versions through v240 are vulnerable.
CVE-2018-16866	An out of bounds read was discovered in systemd-journald in the way it parses log messages that terminate with a colon ':'. A local attacker can use this flaw to disclose process memory data. Versions from v221 to v239 are vulnerable.
CVE-2018-16877	A flaw was found in the way pacemaker's client-server authentication was implemented in versions up to and including 2.0.0. A local attacker could use this flaw, and combine it with other IPC weaknesses, to achieve local privilege escalation.
CVE-2018-16878	A flaw was found in pacemaker up to and including version 2.0.1. An insufficient verification inflicted preference of uncontrolled processes can lead to DoS
CVE-2018-16881	A denial of service vulnerability was found in rsyslog in the imptcp module. An attacker could send a specially crafted message to the imptcp socket, which would cause rsyslog to crash. Versions before 8.27.0 are vulnerable.
CVE-2018-16884	A flaw was found in the Linux kernel's NFS41+ subsystem. NFS41+ shares mounted in different network namespaces at the same time can make bc_svc_process() use wrong back-channel IDs and cause a use-after-free vulnerability. Thus a malicious container user can cause a host kernel memory corruption and a system panic. Due to the nature of the flaw, privilege escalation cannot be fully ruled out.
CVE-2018-16890	libcurl versions from 7.36.0 to before 7.64.0 is vulnerable to a heap buffer out-of-bounds read. The function handling incoming NTLM type-2 messages ('lib/vauth/ntlm.c:ntlm_decode_type2_target') does not validate incoming data correctly and is subject to an integer overflow vulnerability. Using that overflow, a malicious or broken NTLM server could trick libcurl to accept a bad length + offset combination that would lead to a buffer read out-of-bounds.
CVE-2018-17095	An issue has been discovered in mpruett Audio File Library (aka audiofile) 0.3.6, 0.3.5, 0.3.4, 0.3.3, 0.3.2, 0.3.1, 0.3.0. A heap-based buffer overflow in

	Expand3To4Module::run has occurred when running sfconvert.
CVE-2018-17100	An issue was discovered in LibTIFF 4.0.9. There is a int32 overflow in multiply_ms in tools/ppm2tiff.c, which can cause a denial of service (crash) or possibly have unspecified other impact via a crafted image file.
CVE-2018-17101	An issue was discovered in LibTIFF 4.0.9. There are two out-of-bounds writes in cpTags in tools/tiff2bw.c and tools/pal2rgb.c, which can cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image file.
CVE-2018-17182	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.
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-2018-17189	In Apache HTTP server versions 2.4.37 and prior, by sending request bodies in a slow loris way to plain resources, the h2 stream for that request unnecessarily occupied a server thread cleaning up that incoming data. This affects only HTTP/2 (mod_http2) connections.
CVE-2018-17282	An issue was discovered in Exiv2 v0.26. The function Exiv2::DataValue::copy in value.cpp has a NULL pointer dereference.
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-2018-17456	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.

CVE-2018-17462	Incorrect refcounting in AppCache in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to perform a sandbox escape via a crafted HTML page.
CVE-2018-17463	Incorrect side effect annotation in V8 in Google Chrome prior to 70.0.3538.64 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-17464	Incorrect handling of history on iOS in Navigation in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-17465	Incorrect implementation of object trimming in V8 in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2018-17466	Incorrect texture handling in Angle in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-17467	Insufficiently quick clearing of stale rendered content in Navigation in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-17468	Incorrect handling of timer information during navigation in Blink in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to obtain cross origin URLs via a crafted HTML page.
CVE-2018-17469	Incorrect handling of PDF filter chains in PDFium in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2018-17470	A heap buffer overflow in GPU in Google Chrome prior to 70.0.3538.67 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2018-17471	Incorrect dialog placement in WebContents in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to obscure the full screen warning via a crafted HTML page.
CVE-2018-17473	Incorrect handling of confusable characters in Omnibox in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-17474	Use after free in HTMLImportsController in Blink in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-17475	Incorrect handling of history on iOS in Navigation in Google Chrome prior to 70.0.3538.67 allowed a remote

	attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-17476	Incorrect dialog placement in Cast UI in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to obscure the full screen warning via a crafted HTML page.
CVE-2018-17477	Incorrect dialog placement in Extensions in Google Chrome prior to 70.0.3538.67 allowed a remote attacker to spoof the contents of extension popups via a crafted HTML page.
CVE-2018-17478	Incorrect array position calculations in V8 in Google Chrome prior to 70.0.3538.102 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2018-17479	Incorrect object lifetime calculations in GPU code in Google Chrome prior to 70.0.3538.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-17480	Execution of user supplied Javascript during array deserialization leading to an out of bounds write in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-17481	Incorrect object lifecycle handling in PDFium in Google Chrome prior to 71.0.3578.98 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2018-17581	CiffDirectory::readDirectory() at crwimage_int.cpp in Exiv2 0.26 has excessive stack consumption due to a recursive function, leading to Denial of service.
CVE-2018-17828	Directory traversal vulnerability in ZZIPLib 0.13.69 allows attackers to overwrite arbitrary files via a .. (dot dot) in a zip file, because of the function unzzip_cat in the bins/unzzipcat-mem.c file.
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-2018-17972	An issue was discovered in the proc_pid_stack function in fs/proc/base.c in the Linux kernel through 4.18.11. It does not ensure that only root may inspect the kernel stack of an arbitrary task, allowing a local attacker to exploit racy stack unwinding and leak kernel task stack contents.
CVE-2018-18021	arch/arm64/kvm/guest.c in KVM in the Linux kernel before 4.18.12 on the arm64 platform mishandles the KVM_SET_ON_REG ioctl. This is exploitable by attackers who can create virtual machines. An attacker can arbitrarily redirect the hypervisor flow of control

	(with full register control). An attacker can also cause a denial of service (hypervisor panic) via an illegal exception return. This occurs because of insufficient restrictions on userspace access to the core register file, and because PSTATE.M validation does not prevent unintended execution modes.
CVE-2018-18066	snmp_oid_compare in snmplib/snmp_api.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an unauthenticated 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-2018-18074	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.
CVE-2018-18284	Artifex Ghostscript 9.25 and earlier allows attackers to bypass a sandbox protection mechanism via vectors involving the 1Policy operator.
CVE-2018-18310	An invalid memory address dereference was discovered in dwfl_segment_report_module.c in libdwfl in elfutils through v0.174. The vulnerability allows attackers to cause a denial of service (application crash) with a crafted ELF file, as demonstrated by consider_notes.
CVE-2018-18311	Perl before 5.26.3 and 5.28.x before 5.28.1 has a buffer overflow via a crafted regular expression that triggers invalid write operations.
CVE-2018-18335	Heap buffer overflow in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18336	Incorrect object lifecycle in PDFium in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2018-18337	Incorrect handling of stylesheets leading to a use after free in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18338	Incorrect, thread-unsafe use of SkImage in Canvas in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18339	Incorrect object lifecycle in WebAudio in Google Chrome prior to 71.0.3578.80 allowed a remote attacker

	to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18340	Incorrect object lifecycle in MediaRecorder in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18341	An integer overflow leading to a heap buffer overflow in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18342	Execution of user supplied Javascript during object deserialization can update object length leading to an out of bounds write in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-18343	Incorrect handing of paths leading to a use after free in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18344	Inappropriate allowance of the setDownloadBehavior devtools protocol feature in Extensions in Google Chrome prior to 71.0.3578.80 allowed a remote attacker with control of an installed extension to access files on the local file system via a crafted Chrome Extension.
CVE-2018-18345	Incorrect handling of blob URLs in Site Isolation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker who had compromised the renderer process to bypass site isolation protections via a crafted HTML page.
CVE-2018-18346	Incorrect handling of alert box display in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to present confusing browser UI via a crafted HTML page.
CVE-2018-18347	Incorrect handling of failed navigations with invalid URLs in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to trick a user into executing javascript in an arbitrary origin via a crafted HTML page.
CVE-2018-18348	Incorrect handling of bidirectional domain names with RTL characters in Omnibox in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-18349	Remote frame navigations was incorrectly permitted to local resources in Blink in Google Chrome prior to 71.0.3578.80 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system via a crafted Chrome Extension.

CVE-2018-18350	Incorrect handling of CSP enforcement during navigations in Blink in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2018-18351	Lack of proper validation of ancestor frames site when sending lax cookies in Navigation in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to bypass SameSite cookie policy via a crafted HTML page.
CVE-2018-18352	Service works could inappropriately gain access to cross origin audio in Media in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to bypass same origin policy for audio content via a crafted HTML page.
CVE-2018-18353	Failure to dismiss http auth dialogs on navigation in Network Authentication in Google Chrome on Android prior to 71.0.3578.80 allowed a remote attacker to confuse the user about the origin of an auto dialog via a crafted HTML page.
CVE-2018-18354	Insufficient validate of external protocols in Shell Integration in Google Chrome on Windows prior to 71.0.3578.80 allowed a remote attacker to launch external programs via a crafted HTML page.
CVE-2018-18355	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-18356	An integer overflow in path handling lead to a use after free in Skia in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-18357	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-18358	Lack of special casing of localhost in WPAD files in Google Chrome prior to 71.0.3578.80 allowed an attacker on the local network segment to proxy resources on localhost via a crafted WPAD file.
CVE-2018-18359	Incorrect handling of Reflect.construct in V8 in Google Chrome prior to 71.0.3578.80 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-18384	Info-ZIP UnZip 6.0 has a buffer overflow in list.c, when a ZIP archive has a crafted relationship between the compressed-size value and the uncompressed-size value, because a buffer size is 10 and is supposed to be 12.

CVE-2018-18492	A use-after-free vulnerability can occur after deleting a selection element due to a weak reference to the select element in the options collection. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.4, Firefox ESR < 60.4, and Firefox < 64.
CVE-2018-18493	A buffer overflow can occur in the Skia library during buffer offset calculations with hardware accelerated canvas 2D actions due to the use of 32-bit calculations instead of 64-bit. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.4, Firefox ESR < 60.4, and Firefox < 64.
CVE-2018-18494	A same-origin policy violation allowing the theft of cross-origin URL entries when using the Javascript location property to cause a redirection to another site using performance.getEntries(). This is a same-origin policy violation and could allow for data theft. This vulnerability affects Thunderbird < 60.4, Firefox ESR < 60.4, and Firefox < 64.
CVE-2018-18498	A potential vulnerability leading to an integer overflow can occur during buffer size calculations for images when a raw value is used instead of the checked value. This leads to a possible out-of-bounds write. This vulnerability affects Thunderbird < 60.4, Firefox ESR < 60.4, and Firefox < 64.
CVE-2018-18506	When proxy auto-detection is enabled, if a web server serves a Proxy Auto-Configuration (PAC) file or if a PAC file is loaded locally, this PAC file can specify that requests to the localhost are to be sent through the proxy to another server. This behavior is disallowed by default when a proxy is manually configured, but when enabled could allow for attacks on services and tools that bind to the localhost for networked behavior if they are accessed through browsing. This vulnerability affects Firefox < 65.
CVE-2018-18511	Cross-origin images can be read from a canvas element in violation of the same-origin policy using the transferFromImageBitmap method. *Note: This only affects Firefox 65. Previous versions are unaffected.*. This vulnerability affects Firefox < 65.0.1.
CVE-2018-18520	An Invalid Memory Address Dereference exists in the function elf_end in libelf in elfutils through v0.174. Although eu-size is intended to support ar files inside ar files, handle_ar in size.c closes the outer ar file before handling all inner entries. The vulnerability allows attackers to cause a denial of service (application crash) with a crafted ELF file.
CVE-2018-18521	Divide-by-zero vulnerabilities in the function arlib_add_symbols() in arlib.c in elfutils 0.174 allow remote attackers to cause a denial of service

	(application crash) with a crafted ELF file, as demonstrated by eu-ranlib, because a zero sh_entsize is mishandled.
CVE-2018-18544	There is a memory leak in the function WriteMSLImage of coders/msl.c in ImageMagick 7.0.8-13 Q16, and the function ProcessMSLScript of coders/msl.c in GraphicsMagick before 1.3.31.
CVE-2018-18557	LibTIFF 3.9.3, 3.9.4, 3.9.5, 3.9.6, 3.9.7, 4.0.0alpha4, 4.0.0alpha5, 4.0.0alpha6, 4.0.0beta7, 4.0.0, 4.0.1, 4.0.2, 4.0.3, 4.0.4, 4.0.4beta, 4.0.5, 4.0.6, 4.0.7, 4.0.8 and 4.0.9 (with JBIG enabled) decodes arbitrarily-sized JBIG into a buffer, ignoring the buffer size, which leads to a tif_jbig.c JBIGDecode out-of-bounds write.
CVE-2018-18584	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.
CVE-2018-18585	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).
CVE-2018-18661	An issue was discovered in LibTIFF 4.0.9. There is a NULL pointer dereference in the function LZWDecode in the file tif_lzw.c.
CVE-2018-18710	An issue was discovered in the Linux kernel through 4.19. An information leak in cdrom_ioctl_select_disc 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 and CVE-2018-16658.
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-2018-18897	An issue was discovered in Poppler 0.71.0. There is a memory leak in GfxColorSpace::setDisplayProfile in GfxState.cc, as demonstrated by pdftocairo.
CVE-2018-18915	There is an infinite loop in the Exiv2::Image::printIFDStructure function of image.cpp in Exiv2 0.27-RC1. A crafted input will lead to a remote denial of service attack.
CVE-2018-19044	keepalived 2.0.8 didn't check for pathnames with symlinks when writing data to a temporary file upon a call to PrintData or PrintStats. This allowed local users to overwrite arbitrary files if fs.protected_symlinks is set to 0, as demonstrated by a symlink from /tmp/keepalived.data or /tmp/keepalived.stats to /etc/passwd.
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-2018-19107	In Exiv2 0.26, Exiv2::IptcParser::decode in iptc.cpp (called from psdimage.cpp in the PSD image reader) may suffer from a denial of service (heap-based buffer over-read) caused by an integer overflow via a crafted PSD image file.
CVE-2018-19108	In Exiv2 0.26, Exiv2::PsdImage::readMetadata in psdimage.cpp in the PSD image reader may suffer from a denial of service (infinite loop) caused by an integer overflow via a crafted PSD image file.
CVE-2018-19115	keepalived before 2.0.7 has a heap-based buffer overflow when parsing HTTP status codes resulting in DoS or possibly unspecified other impact, because extract_status_code in lib/html.c has no validation of the status code and instead writes an unlimited amount of data to the heap.
CVE-2018-19134	In Artifex Ghostscript through 9.25, the setpattern operator did not properly validate certain types. A specially crafted PostScript document could exploit this to crash Ghostscript or, possibly, execute arbitrary code in the context of the Ghostscript process. This is a type confusion issue because of failure to check whether the Implementation of a pattern dictionary was a structure type.
CVE-2018-19149	Poppler before 0.70.0 has a NULL pointer dereference in _poppler_attachment_new when called from poppler_annot_file_attachment_get_attachment.
CVE-2018-19198	An issue was discovered in uriparser before 0.9.0. UriQuery.c allows an out-of-bounds write via a uriComposeQuery* or uriComposeQueryEx* function because the '&' character is mishandled in certain contexts.
CVE-2018-19199	An issue was discovered in uriparser before 0.9.0. UriQuery.c allows an integer overflow via a uriComposeQuery* or uriComposeQueryEx* function because of an unchecked multiplication.
CVE-2018-19208	In libwpd 0.10.2, there is a NULL pointer dereference in the function WP6ContentListener::defineTable in

	WP6ContentListener.cpp that will lead to a denial of service attack. This is related to WPXTable.h.
CVE-2018-1922	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is affected by buffer overflow vulnerability that can potentially result in arbitrary code execution. IBM X-Force ID: 152858.
CVE-2018-1923	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is affected by buffer overflow vulnerability that can potentially result in arbitrary code execution. IBM X-Force ID: 152859.
CVE-2018-19407	The vcpu_scan_ioapic function in arch/x86/kvm/x86.c in the Linux kernel through 4.19.2 allows local users to cause a denial of service (NULL pointer dereference and BUG) via crafted system calls that reach a situation where ioapic is uninitialized.
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-2018-19486	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.
CVE-2018-19519	In tcpdump 4.9.2, a stack-based buffer over-read exists in the print_prefix function of print-hncp.c via crafted packet data because of missing initialization.
CVE-2018-19535	In Exiv2 0.26 and previous versions, PngChunk::readRawProfile in pngchunk_int.cpp may cause a denial of service (application crash due to a heap-based buffer over-read) via a crafted PNG file.
CVE-2018-19591	In the GNU C Library (aka glibc or libc6) through 2.28, attempting to resolve a crafted hostname via getaddrinfo() leads to the allocation of a socket descriptor that is not closed. This is related to the if_name_to_index() function.
CVE-2018-19607	Exiv2::isoSpeed in easyaccess.cpp in Exiv2 v0.27-RC2 allows remote attackers to cause a denial of service

	(NULL pointer dereference and application crash) via a crafted file.
CVE-2018-19622	In Wireshark 2.6.0 to 2.6.4 and 2.4.0 to 2.4.10, the MMSE dissector could go into an infinite loop. This was addressed in epan/dissectors/packet-mmse.c by preventing length overflows.
CVE-2018-19662	An issue was discovered in libsndfile 1.0.28. There is a buffer over-read in the function i2alaw_array in alaw.c that will lead to a denial of service.
CVE-2018-1978	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-ForceID: 154069.
CVE-2018-19788	A flaw was found in PolicyKit (aka polkit) 0.115 that allows a user with a uid greater than INT_MAX to successfully execute any systemctl command.
CVE-2018-1980	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-ForceID: 154078.
CVE-2018-19869	An issue was discovered in Qt before 5.11.3. A malformed SVG image causes a segmentation fault in qsvghandler.cpp.
CVE-2018-19870	An issue was discovered in Qt before 5.11.3. A malformed GIF image causes a NULL pointer dereference in QGifHandler resulting in a segmentation fault.
CVE-2018-19871	An issue was discovered in Qt before 5.11.3. There is QTgaFile Uncontrolled Resource Consumption.
CVE-2018-19872	An issue was discovered in Qt 5.11. A malformed PPM image causes a division by zero and a crash in qppmhandler.cpp.
CVE-2018-19873	An issue was discovered in Qt before 5.11.3. QBmpHandler has a buffer overflow via BMP data.
CVE-2018-20060	urllib3 before version 1.23 does not remove the Authorization HTTP header when following a cross-origin redirect (i.e., a redirect that differs in host, port, or scheme). This can allow for credentials in the Authorization header to be exposed to unintended hosts or transmitted in cleartext.
CVE-2018-20096	There is a heap-based buffer over-read in the Exiv2::tEXtToDataBuf function of pngimage.cpp in Exiv2 0.27-RC3. A crafted input will lead to a remote denial of service attack.
CVE-2018-20097	There is a SEGV in Exiv2::Internal::TiffParserWorker::findPrimaryGroups of

	tiffimage_int.cpp in Exiv2 0.27-RC3. A crafted input will lead to a remote denial of service attack.
CVE-2018-20098	There is a heap-based buffer over-read in Exiv2::Jp2Image::encodeJp2Header of jp2image.cpp in Exiv2 0.27-RC3. A crafted input will lead to a remote denial of service attack.
CVE-2018-20099	There is an infinite loop in Exiv2::Jp2Image::encodeJp2Header of jp2image.cpp in Exiv2 0.27-RC3. A crafted input will lead to a remote denial of service attack.
CVE-2018-20169	An issue was discovered in the Linux kernel before 4.19.9. The USB subsystem mishandles size checks during the reading of an extra descriptor, related to __usb_get_extra_descriptor in drivers/usb/core/usb.c.
CVE-2018-20226	An organization administrator can add a super administrator in THEHIVE PROJECT Cortex before 2.1.3 due to the lack of overriding the Role.toString method.
CVE-2018-20406	Modules/_pickle.c in Python before 3.7.1 has an integer overflow via a large LONG_BINPUT value that is mishandled during a "resize to twice the size" attempt. This issue might cause memory exhaustion, but is only relevant if the pickle format is used for serializing tens or hundreds of gigabytes of data. This issue is fixed in: v3.4.10, v3.4.10rc1; v3.5.10, v3.5.10rc1, v3.5.7, v3.5.7rc1, v3.5.8, v3.5.8rc1, v3.5.8rc2, v3.5.9; v3.6.10, v3.6.10rc1, v3.6.11, v3.6.11rc1, v3.6.12, v3.6.7, v3.6.7rc1, v3.6.7rc2, v3.6.8, v3.6.8rc1, v3.6.9, v3.6.9rc1; v3.7.1, v3.7.1rc1, v3.7.1rc2, v3.7.2, v3.7.2rc1, v3.7.3, v3.7.3rc1, v3.7.4, v3.7.4rc1, v3.7.4rc2, v3.7.5, v3.7.5rc1, v3.7.6, v3.7.6rc1, v3.7.7, v3.7.7rc1, v3.7.8, v3.7.8rc1, v3.7.9.
CVE-2018-20467	In coders/bmp.c in ImageMagick before 7.0.8-16, an input file can result in an infinite loop and hang, with high CPU and memory consumption. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted file.
CVE-2018-20481	XRef::getEntry in XRef.cc in Poppler 0.72.0 mishandles unallocated XRef entries, which allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted PDF document, when XRefEntry::setFlag in XRef.h is called from Parser::makeStream in Parser.cc.
CVE-2018-20483	set_file_metadata in xattr.c in GNU Wget before 1.20.1 stores a file's origin URL in the user.xdg.origin.url metadata attribute of the extended attributes of the downloaded file, which allows local users to obtain sensitive information (e.g., credentials contained in the URL) by reading this attribute, as demonstrated by getfattr. This also applies to Referer information in the

	user.xdg.referrer.url metadata attribute. According to 2016-07-22 in the Wget ChangeLog, user.xdg.origin.url was partially based on the behavior of fwrite_xattr in tool_xattr.c in curl.
CVE-2018-20532	There is a NULL pointer dereference at ext/testcase.c (function testcase_read) in libsolvext.a in libsolv through 0.7.2 that will cause a denial of service.
CVE-2018-20533	There is a NULL pointer dereference at ext/testcase.c (function testcase_str2dep_complex) in libsolvext.a in libsolv through 0.7.2 that will cause a denial of service.
CVE-2018-20534	** DISPUTED ** There is an illegal address access at ext/testcase.c in libsolv.a in libsolv through 0.7.2 that will cause a denial of service. NOTE: third parties dispute this issue stating that the issue affects the test suite and not the underlying library. It cannot be exploited in any real-world application.
CVE-2018-20650	A reachable Object::dictLookup assertion in Poppler 0.72.0 allows attackers to cause a denial of service due to the lack of a check for the dict data type, as demonstrated by use of the FileSpec class (in FileSpec.cc) in pdfdetach.
CVE-2018-20662	In Poppler 0.72.0, PDFDoc::setup in PDFDoc.cc allows attackers to cause a denial-of-service (application crash caused by Object.h SIGABRT, because of a wrong return value from PDFDoc::setup) by crafting a PDF file in which an xref data structure is mishandled during extractPDFSubtype processing.
CVE-2018-20669	An issue where a provided address with access_ok() is not checked was discovered in i915_gem_execbuffer2_ioctl in drivers/gpu/drm/i915/i915_gem_execbuffer.c in the Linux kernel through 4.19.13. A local attacker can craft a malicious IOCTL function call to overwrite arbitrary kernel memory, resulting in a Denial of Service or privilege escalation.
CVE-2018-20676	In Bootstrap before 3.4.0, XSS is possible in the tooltip data-viewport attribute.
CVE-2018-20677	In Bootstrap before 3.4.0, XSS is possible in the affix configuration target property.
CVE-2018-20685	In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.
CVE-2018-20699	Docker Engine before 18.09 allows attackers to cause a denial of service (dockerd memory consumption) via a large integer in a --cpuset-mems or --cpuset-cpus value, related to daemon/daemon_unix.go, pkg/parsers/parsers.go, and pkg/sysinfo/sysinfo.go.

CVE-2018-20815	In QEMU 3.1.0, <code>load_device_tree</code> in <code>device_tree.c</code> calls the deprecated <code>load_image</code> function, which has a buffer overflow risk.
CVE-2018-20843	In libexpat in Expat before 2.2.7, XML input including XML names that contain a large number of colons could make the XML parser consume a high amount of RAM and CPU resources while processing (enough to be usable for denial-of-service attacks).
CVE-2018-20845	Division-by-zero vulnerabilities in the functions <code>pi_next_pcrl</code> , <code>pi_next_cprl</code> , and <code>pi_next_rpcl</code> in <code>openmj2/pi.c</code> in OpenJPEG through 2.3.0 allow remote attackers to cause a denial of service (application crash).
CVE-2018-20847	An improper computation of <code>p_tx0</code> , <code>p_tx1</code> , <code>p_ty0</code> and <code>p_ty1</code> in the function <code>opj_get_encoding_parameters</code> in <code>openjp2/pi.c</code> in OpenJPEG through 2.3.0 can lead to an integer overflow.
CVE-2018-20852	<code>http.cookiejar.DefaultPolicy.domain_return_ok</code> in <code>Lib/http/cookiejar.py</code> in Python before 3.7.3 does not correctly validate the domain: it can be tricked into sending existing cookies to the wrong server. An attacker may abuse this flaw by using a server with a hostname that has another valid hostname as a suffix (e.g., <code>pythonicexample.com</code> to steal cookies for <code>example.com</code>). When a program uses <code>http.cookiejar.DefaultPolicy</code> and tries to do an HTTP connection to an attacker-controlled server, existing cookies can be leaked to the attacker. This affects 2.x through 2.7.16, 3.x before 3.4.10, 3.5.x before 3.5.7, 3.6.x before 3.6.9, and 3.7.x before 3.7.3.
CVE-2018-20969	<code>do_ed_script</code> in <code>pch.c</code> in GNU patch through 2.7.6 does not block strings beginning with a ! character. NOTE: this is the same commit as for CVE-2019-13638, but the ! syntax is specific to ed, and is unrelated to a shell metacharacter.
CVE-2018-21009	Poppler before 0.66.0 has an integer overflow in <code>Parser::makeStream</code> in <code>Parser.cc</code> .
CVE-2018-25011	A heap-based buffer overflow was found in libwebp in versions before 1.0.1 in <code>PutLE16()</code> .
CVE-2018-25014	A use of uninitialized value was found in libwebp in versions before 1.0.1 in <code>ReadSymbol()</code> .
CVE-2018-25020	The BPF subsystem in the Linux kernel before 4.17 mishandles situations with a long jump over an instruction sequence where inner instructions require substantial expansions into multiple BPF instructions, leading to an overflow. This affects <code>kernel/bpf/core.c</code> and <code>net/core/filter.c</code> .
CVE-2018-25032	zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches.

CVE-2018-2562	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Partition). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.19 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server 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-2018-2579	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. 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 read access to a subset of Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2018-2582	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 8u152 and 9.0.1; Java SE Embedded: 8u151. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability 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 6.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N).
CVE-2018-2588	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: LDAP). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).
CVE-2018-2599	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. 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 update, insert or delete access to some 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 client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 4.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L).
CVE-2018-2602	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: I18n). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure

	<p>where Java SE, Java SE Embedded executes to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:L).</p>
CVE-2018-2603	<p>Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).</p>
CVE-2018-2618	<p>Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JCE). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java</p>

	<p>SE, Java SE Embedded, JRockit accessible data.</p> <p>Note: This vulnerability 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).</p>
CVE-2018-2622	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2629	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JGSS). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. 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. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N).
CVE-2018-2633	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Difficult to exploit vulnerability allows unauthenticated attacker with

	<p>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 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 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).</p>
CVE-2018-2634	<p>Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JGSS). Supported versions that are affected are Java SE: 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).</p>
CVE-2018-2637	<p>Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JMX). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. 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 creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit accessible data as well as unauthorized access to critical data or</p>

	complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 7.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N).
CVE-2018-2640	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2641	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151. 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 creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 6.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:N).
CVE-2018-2663	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable 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. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L).
CVE-2018-2665	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2668	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2677	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments,

	typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L).
CVE-2018-2678	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u171, 7u161, 8u152 and 9.0.1; Java SE Embedded: 8u151; JRockit: R28.3.16. Easily exploitable 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. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 4.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L).
CVE-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-2018-2761	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-2018-2765	Vulnerability in the Oracle Security Service component of Oracle Fusion Middleware (subcomponent: Oracle SSL API). Supported versions that are affected are 11.1.1.9.0, 12.1.3.0.0, 12.2.1.2.0 and 12.2.1.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Oracle Security Service. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Security Service accessible data. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2018-2767	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-2018-2771	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-2018-2781	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-2018-2790	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2018-2794	Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162, 10 and JRockit: R28.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, JRockit executes to compromise Java SE, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2018-2795	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated

	<p>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 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).</p>
CVE-2018-2796	<p>Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Concurrency). Supported versions that are affected are Java SE: 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).</p>
CVE-2018-2797	<p>Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JMX). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score</p>

	5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2018-2798	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2018-2799	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2018-2800	Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u181, 7u171 and 8u162; JRockit: R28.3.17. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, JRockit. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to

	some of Java SE, JRockit accessible data as well as unauthorized read access to a subset of Java SE, JRockit accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N).
CVE-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-2018-2814	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H:I:H/A:H).
CVE-2018-2815	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u181, 7u171, 8u162 and 10; Java SE Embedded: 8u161; JRockit: R28.3.17. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit.

	<p>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 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).</p>
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-2018-2819	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-2018-2952	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-2018-3058	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-2018-3063	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-2018-3066	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-2018-3081	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-2018-3136	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-2018-3149	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-2018-3169	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-2018-3174	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

	<p>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).</p>
CVE-2018-3180	<p>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).</p>
CVE-2018-3183	<p>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.</p>

	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-2018-3214	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Sound). Supported versions that are affected are Java SE: 6u201, 7u191 and 8u182; Java SE Embedded: 8u181; JRockit: R28.3.19. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-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-2018-3613	Logic issue in variable service module for EDK II/UDK2018/UDK2017/UDK2015 may allow an authenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via local access.
CVE-2018-3615	Systems with microprocessors utilizing speculative execution and Intel software guard extensions (Intel SGX) may allow unauthorized disclosure of information residing in the L1 data cache from an enclave to an attacker with local user access via a side-channel analysis.

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-2018-3646	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-2018-4871	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-2018-5146	An out of bounds memory write while processing Vorbis audio data was reported through the Pwn2Own contest. This vulnerability affects Firefox < 59.0.1, Firefox ESR < 52.7.2, and Thunderbird < 52.7.
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-2018-5154	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-2018-5159	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-2018-5161	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-2018-5168	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-2018-5170	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-2018-5178	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	A service worker can send the activate event on itself periodically which allows it to run perpetually, allowing it to monitor activity by users. Affects all versions prior to Firefox 60.
CVE-2018-5183	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-2018-5188	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-2018-5344	In the Linux kernel through 4.14.13, drivers/block/loop.c mishandles lo_release serialization, which allows attackers to cause a denial of service (_lock_acquire use-after-free) or possibly have unspecified other impact.
CVE-2018-5390	Linux kernel versions 4.9+ can be forced to make very expensive calls to tcpCollapseOfoQueue() and tcpPruneOfoQueue() 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-2018-5407	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'.
CVE-2018-5683	The vga_draw_text function in Qemu allows local OS guest privileged users to cause a denial of service (out-of-bounds read and QEMU process crash) by leveraging improper memory address validation.
CVE-2018-5727	In OpenJPEG 2.3.0, there is an integer overflow vulnerability in the opj_t1_encode_cblk function (openjp2/t1.c). Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file.
CVE-2018-5729	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos database to cause a denial of service (NULL pointer dereference) or bypass a DN container check by supplying tagged data that is internal to the database module.
CVE-2018-5730	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos database to circumvent a DN containership check by supplying both a "linkdn" and "containerdn" database argument, or by supplying a DN string which is a left extension of a container DN string but is not hierarchically within the container DN.
CVE-2018-5732	Failure to properly bounds-check a buffer used for processing DHCP options allows a malicious server (or an entity masquerading as a server) to cause a buffer

	overflow (and resulting crash) in dhclient by sending a response containing a specially constructed options section. Affects ISC DHCP versions 4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0
CVE-2018-5733	A malicious client which is allowed to send very large amounts of traffic (billions of packets) to a DHCP server can eventually overflow a 32-bit reference counter, potentially causing dhcpd to crash. Affects ISC DHCP 4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0.
CVE-2018-5740	"deny-answer-aliases" is a little-used feature intended to help recursive server operators protect end users against DNS rebinding attacks, a potential method of circumventing the security model used by client browsers. However, a defect in this feature makes it easy, when the feature is in use, to experience an assertion failure in name.c. Affects BIND 9.7.0->9.8.8, 9.9.0->9.9.13, 9.10.0->9.10.8, 9.11.0->9.11.4, 9.12.0->9.12.2, 9.13.0->9.13.2.
CVE-2018-5741	To provide fine-grained controls over the ability to use Dynamic DNS (DDNS) to update records in a zone, BIND 9 provides a feature called update-policy. Various rules can be configured to limit the types of updates that can be performed by a client, depending on the key used when sending the update request. Unfortunately, some rule types were not initially documented, and when documentation for them was added to the Administrator Reference Manual (ARM) in change #3112, the language that was added to the ARM at that time incorrectly described the behavior of two rule types, krb5-subdomain and ms-subdomain. This incorrect documentation could mislead operators into believing that policies they had configured were more restrictive than they actually were. This affects BIND versions prior to BIND 9.11.5 and BIND 9.12.3.
CVE-2018-5742	While backporting a feature for a newer branch of BIND9, RedHat introduced a path leading to an assertion failure in buffer.c:420. Affects RedHat versions bind-9.9.4-65.el7 -> bind-9.9.4-72.el7. No ISC releases are affected. Other packages from other distributions who made the same error may also be affected.
CVE-2018-5743	By design, BIND is intended to limit the number of TCP clients that can be connected at any given time. The number of allowed connections is a tunable parameter which, if unset, defaults to a conservative value for most servers. Unfortunately, the code which was intended to limit the number of simultaneous connections contained an error which could be exploited to grow the number of simultaneous connections beyond this limit. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.6,

	9.12.0 -> 9.12.4, 9.14.0. BIND 9 Supported Preview Edition versions 9.9.3-S1 -> 9.11.5-S3, and 9.11.5-S5. Versions 9.13.0 -> 9.13.7 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2018-5743.
CVE-2018-5745	"managed-keys" is a feature which allows a BIND resolver to automatically maintain the keys used by trust anchors which operators configure for use in DNSSEC validation. Due to an error in the managed-keys feature it is possible for a BIND server which uses managed-keys to exit due to an assertion failure if, during key rollover, a trust anchor's keys are replaced with keys which use an unsupported algorithm. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.5-P1, 9.12.0 -> 9.12.3-P1, and versions 9.9.3-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2018-5745.
CVE-2018-5748	qemu/qemu_monitor.c in libvirt allows attackers to cause a denial of service (memory consumption) via a large QEMU reply.
CVE-2018-5750	The acpi_smbus_hc_add function in drivers/acpi/sbshc.c in the Linux kernel through 4.14.15 allows local users to obtain sensitive address information by reading dmesg data from an SBS HC printk call.
CVE-2018-5785	In OpenJPEG 2.3.0, there is an integer overflow caused by an out-of-bounds left shift in the opj_j2k_setup_encoder function (openjp2/j2k.c). Remote attackers could leverage this vulnerability to cause a denial of service via a crafted bmp file.
CVE-2018-5950	Cross-site scripting (XSS) vulnerability in the web UI in Mailman before 2.1.26 allows remote attackers to inject arbitrary web script or HTML via a user-options URL.
CVE-2018-6031	Use after free in PDFium in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2018-6032	Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user cross-origin data via a crafted HTML page.
CVE-2018-6033	Insufficient data validation in Downloads in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially run arbitrary code outside sandbox via a crafted Chrome Extension.
CVE-2018-6034	Insufficient data validation in WebGL in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to

	perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6035	Insufficient policy enforcement in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user local file data via a crafted Chrome Extension.
CVE-2018-6036	Insufficient data validation in V8 in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user data via a crafted HTML page.
CVE-2018-6037	Inappropriate implementation in autofill in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to obtain autofill data with insufficient user gestures via a crafted HTML page.
CVE-2018-6038	Heap buffer overflow in WebGL in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6039	Insufficient data validation in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user cross-origin data via a crafted Chrome Extension.
CVE-2018-6040	Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially bypass content security policy via a crafted HTML page.
CVE-2018-6041	Incorrect security UI in navigation in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6042	Incorrect security UI in Omnibox in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6043	Insufficient data validation in External Protocol Handler in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially execute arbitrary programs on user machine via a crafted HTML page.
CVE-2018-6044	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6045	Insufficient policy enforcement in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user local file data via a crafted Chrome Extension.
CVE-2018-6046	Insufficient data validation in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote

	attacker to potentially leak user cross-origin data via a crafted Chrome Extension.
CVE-2018-6047	Insufficient policy enforcement in WebGL in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user redirect URL via a crafted HTML page.
CVE-2018-6048	Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak referrer information via a crafted HTML page.
CVE-2018-6049	Incorrect security UI in permissions prompt in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the origin to which permission is granted via a crafted HTML page.
CVE-2018-6050	Incorrect security UI in Omnibox in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6051	XSS Auditor in Google Chrome prior to 64.0.3282.119, did not ensure the reporting URL was in the same origin as the page it was on, which allowed a remote attacker to obtain referrer details via a crafted HTML page.
CVE-2018-6052	Lack of support for a non standard no-referrer policy value in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to obtain referrer details from a web page that had thought it had opted out of sending referrer data.
CVE-2018-6053	Inappropriate implementation in New Tab Page in Google Chrome prior to 64.0.3282.119 allowed a local attacker to view website thumbnail images after clearing browser data via a crafted HTML page.
CVE-2018-6054	Use after free in WebUI in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2018-6055	Insufficient policy enforcement in Catalog Service in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially run arbitrary code outside sandbox via a crafted HTML page.
CVE-2018-6056	Type confusion could lead to a heap out-of-bounds write in V8 in Google Chrome prior to 64.0.3282.168 allowing a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-6057	Lack of special casing of Android ashmem in Google Chrome prior to 65.0.3325.146 allowed a remote attacker who had compromised the renderer process to bypass inter-process read only guarantees via a crafted HTML page.

CVE-2018-6060	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 <code>__defineGetter__</code> 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 Blink in Google Chrome prior to 65.0.3325.146 allowed an attacker who convinced a user to install a malicious extension to bypass content security policy via a crafted Chrome Extension.
CVE-2018-6071	An integer overflow in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6072	An integer overflow leading to use after free in PDFium in Google Chrome prior to 65.0.3325.146 allowed a

	remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2018-6073	A heap buffer overflow in WebGL in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6074	Failure to apply Mark-of-the-Web in Downloads in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to bypass OS level controls via a crafted HTML page.
CVE-2018-6075	Incorrect handling of specified filenames in file downloads in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page and user interaction.
CVE-2018-6076	Insufficient encoding of URL fragment identifiers in Blink in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform a DOM based XSS attack via a crafted HTML page.
CVE-2018-6077	Displacement map filters being applied to cross-origin images in Blink SVG rendering in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6078	Incorrect handling of confusable characters in Omnibox in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-6079	Inappropriate sharing of TEXTURE_2D_ARRAY/TEXTURE_3D data between tabs in WebGL in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6080	Lack of access control checks in Instrumentation in Google Chrome prior to 65.0.3325.146 allowed a remote attacker who had compromised the renderer process to obtain memory metadata from privileged processes .
CVE-2018-6081	XSS vulnerabilities in Interstitials in Google Chrome prior to 65.0.3325.146 allowed an attacker who convinced a user to install a malicious extension or open Developer Console to inject arbitrary scripts or HTML via a crafted HTML page.
CVE-2018-6082	Including port 22 in the list of allowed FTP ports in Networking in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially enumerate internal host services via a crafted HTML page.
CVE-2018-6083	Failure to disallow PWA installation from CSP sandboxed pages in AppManifest in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to access privileged APIs via a crafted HTML page.

CVE-2018-6085	Re-entry of a destructor in Networking Disk Cache in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2018-6086	A double-eviction in the Incognito mode cache that lead to a user-after-free in Networking Disk Cache in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2018-6087	A use-after-free in WebAssembly in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-6088	An iterator-validation bug in PDFium in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.
CVE-2018-6089	A lack of CORS checks, after a Service Worker redirected to a cross-origin PDF, in Service Worker in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak limited cross-origin data via a crafted HTML page.
CVE-2018-6090	An integer overflow that lead to a heap buffer-overflow in Skia in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-6091	Service Workers can intercept any request made by an <embed> or <object> tag in Fetch API in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6092	An integer overflow on 32-bit systems in WebAssembly in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-6093	Insufficient origin checks in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6094	Inline metadata in GarbageCollection in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6095	Inappropriate dismissal of file picker on keyboard events in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to read local files via a crafted HTML page.
CVE-2018-6096	A JavaScript focused window could overlap the fullscreen notification in Fullscreen in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to

	obscure the full screen warning via a crafted HTML page.
CVE-2018-6097	Incorrect handling of asynchronous methods in Fullscreen in Google Chrome on macOS prior to 66.0.3359.117 allowed a remote attacker to enter full screen without showing a warning via a crafted HTML page.
CVE-2018-6098	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6099	A lack of CORS checks in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak limited cross-origin data via a crafted HTML page.
CVE-2018-6100	Incorrect handling of confusable characters in URL Formatter in Google Chrome on macOS prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6101	A lack of host validation in DevTools in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code via a crafted HTML page, if the user is running a remote DevTools debugging server.
CVE-2018-6102	Missing confusable characters in Internationalization in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-6103	A stagnant permission prompt in Prompts in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to bypass permission policy via a crafted HTML page.
CVE-2018-6104	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6105	Incorrect handling of confusable characters in Omnibox in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6106	An asynchronous generator may return an incorrect state in V8 in Google Chrome prior to 66.0.3359.117 allowing a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2018-6107	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6108	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117

	allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted HTML page.
CVE-2018-6109	readAsText() can indefinitely read the file picked by the user, rather than only once at the time the file is picked in File API in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to access data on the user file system without explicit consent via a crafted HTML page.
CVE-2018-6110	Parsing documents as HTML in Downloads in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to cause Chrome to execute scripts via a local non-HTML page.
CVE-2018-6111	An object lifetime issue in the developer tools network handler in Google Chrome prior to 66.0.3359.117 allowed a local attacker to execute arbitrary code via a crafted HTML page.
CVE-2018-6112	Making URLs clickable and allowing them to be styled in DevTools in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2018-6113	Improper handling of pending navigation entries in Navigation in Google Chrome on iOS prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2018-6114	Incorrect enforcement of CSP for <object> tags in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2018-6115	Inappropriate setting of the SEE_MASK_FLAG_NO_UI flag in file downloads in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to potentially bypass OS malware checks via a crafted HTML page.
CVE-2018-6116	A nullptr dereference in WebAssembly in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2018-6117	Confusing settings in Autofill in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2018-6119	Incorrect security UI in Omnibox in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6120	An integer overflow that could lead to an attacker-controlled heap out-of-bounds write in PDFium in Google Chrome prior to 66.0.3359.170 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.

CVE-2018-6121	Insufficient validation of input in Blink in Google Chrome prior to 66.0.3359.170 allowed a remote attacker to perform privilege escalation via a crafted HTML page.
CVE-2018-6122	Type confusion in WebAssembly in Google Chrome prior to 66.0.3359.139 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6123	A use after free in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6124	Type confusion in ReadableStreams in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2018-6125	Insufficient policy enforcement in USB in Google Chrome on Windows prior to 67.0.3396.62 allowed a remote attacker to obtain potentially sensitive information via a crafted HTML page.
CVE-2018-6126	A precision error in Skia in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6127	Early free of object in use in IndexDB in Google Chrome prior to 67.0.3396.62 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2018-6128	Incorrect URL parsing in WebKit in Google Chrome on iOS prior to 67.0.3396.62 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2018-6129	Out of bounds array access in WebRTC in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2018-6130	Incorrect handling of object lifetimes in WebRTC in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2018-6131	Object lifecycle issue in WebAssembly in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6132	Uninitialized data in WebRTC in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted video file.
CVE-2018-6133	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 67.0.3396.62

	allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6134	Information leak in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to bypass no-referrer policy via a crafted HTML page.
CVE-2018-6135	Lack of clearing the previous site before loading alerts from a new one in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2018-6136	Missing type check in V8 in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6137	CSS Paint API in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6138	Insufficient policy enforcement in Extensions API in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.
CVE-2018-6139	Insufficient target checks on the chrome.debugger API in DevTools in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.
CVE-2018-6140	Allowing the chrome.debugger API to attach to Web UI pages in DevTools in Google Chrome prior to 67.0.3396.62 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.
CVE-2018-6141	Insufficient validation of an image filter in Skia in Google Chrome prior to 67.0.3396.62 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6142	Array bounds check failure in V8 in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2018-6143	Insufficient validation in V8 in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6144	Off-by-one error in PDFium in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory write via a crafted PDF file.
CVE-2018-6145	Insufficient data validation in HTML parser in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to bypass same origin policy via a crafted HTML page.

CVE-2018-6147	Lack of secure text entry mode in Browser UI in Google Chrome on Mac prior to 67.0.3396.62 allowed a local attacker to obtain potentially sensitive information from process memory via a local process.
CVE-2018-6148	Incorrect implementation in Content Security Policy in Google Chrome prior to 67.0.3396.79 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2018-6149	Type confusion in JavaScript in Google Chrome prior to 67.0.3396.87 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6150	Incorrect handling of CORS in ServiceWorker in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6151	Bad cast in DevTools in Google Chrome on Win, Linux, Mac, Chrome OS prior to 66.0.3359.117 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted Chrome Extension.
CVE-2018-6152	The implementation of the Page.downloadBehavior backend unconditionally marked downloaded files as safe, regardless of file type in Google Chrome prior to 66.0.3359.117 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted HTML page and user interaction.
CVE-2018-6153	A precision error in Skia in Google Chrome prior to 68.0.3440.75 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6154	Insufficient data validation in WebGL in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6155	Incorrect handling of frames in the VP8 parser in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2018-6156	Incorect derivation of a packet length in WebRTC in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2018-6157	Type confusion in WebRTC in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2018-6158	A race condition in Oilpan in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2018-6159	Insufficient policy enforcement in ServiceWorker in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2018-6161	Insufficient policy enforcement in Blink in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to bypass same origin policy via a crafted HTML page.
CVE-2018-6162	Improper deserialization in WebGL in Google Chrome on Mac prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6163	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6164	Insufficient origin checks for CSS content in Blink in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6165	Incorrect handling of reloads in Navigation in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6166	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6167	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6168	Information leak in media engine in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2018-6169	Lack of timeout on extension install prompt in Extensions in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to trigger installation of an unwanted extension via a crafted HTML page.
CVE-2018-6170	A bad cast in PDFium in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2018-6171	Use after free in Bluetooth in Google Chrome prior to 68.0.3440.75 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory via a crafted Chrome Extension.
CVE-2018-6172	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75

	allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6173	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6174	Integer overflows in Swiftshader in Google Chrome prior to 68.0.3440.75 potentially allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2018-6175	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6176	Insufficient file type enforcement in Extensions API in Google Chrome prior to 68.0.3440.75 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted Chrome Extension.
CVE-2018-6177	Information leak in media engine in Google Chrome prior to 68.0.3440.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6178	Eliding from the wrong side in an infobar in DevTools in Google Chrome prior to 68.0.3440.75 allowed an attacker who convinced a user to install a malicious extension to Hide Chrome Security UI via a crafted Chrome Extension.
CVE-2018-6179	Insufficient enforcement of file access permission in the activeTab case in Extensions in Google Chrome prior to 68.0.3440.75 allowed an attacker who convinced a user to install a malicious extension to access files on the local file system via a crafted Chrome Extension.
CVE-2018-6323	The <code>elf_object_p</code> function in <code>elfcode.h</code> in the Binary File Descriptor (BFD) library (aka <code>libbfd</code>), as distributed in GNU Binutils 2.29.1, has an unsigned integer overflow because <code>bfd_size_type</code> multiplication is not used. A crafted ELF file allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact.
CVE-2018-6485	An integer overflow in the implementation of the <code>posix_memalign</code> in <code>memalign</code> functions in the GNU C Library (aka glibc or libc6) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption.
CVE-2018-6541	In ZZIPlib 0.13.67, there is a bus error caused by loading of a misaligned address (when handling <code>disk64_trailer</code> local entries) in <code>__zzip_fetch_disk_trailer</code> (<code>zzip/zip.c</code>). Remote attackers could leverage this

	vulnerability to cause a denial of service via a crafted zip file.
CVE-2018-6551	The malloc implementation in the GNU C Library (aka glibc or libc6), from version 2.24 to 2.26 on powerpc, and only in version 2.26 on i386, did not properly handle malloc calls with arguments close to SIZE_MAX and could return a pointer to a heap region that is smaller than requested, eventually leading to heap corruption.
CVE-2018-6560	In dbus-proxy/flatpak-proxy.c in Flatpak before 0.8.9, and 0.9.x and 0.10.x before 0.10.3, crafted D-Bus messages to the host can be used to break out of the sandbox, because whitespace handling in the proxy is not identical to whitespace handling in the daemon.
CVE-2018-6574	Go before 1.8.7, Go 1.9.x before 1.9.4, and Go 1.10 pre-releases before Go 1.10rc2 allow "go get" remote command execution during source code build, by leveraging the gcc or clang plugin feature, because -fplugin= and -plugin= arguments were not blocked.
CVE-2018-6764	util/virlog.c in libvirt does not properly determine the hostname on LXC container startup, which allows local guest OS users to bypass an intended container protection mechanism and execute arbitrary commands via a crafted NSS module.
CVE-2018-6914	Directory traversal vulnerability in the Dir.mktmpdir method in the tmpdir library in Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1 might allow attackers to create arbitrary directories or files via a .. (dot dot) in the prefix argument.
CVE-2018-6952	A double free exists in the another_hunk function in pch.c in GNU patch through 2.7.6.
CVE-2018-7159	The HTTP parser in all current versions of Node.js ignores spaces in the `Content-Length` header, allowing input such as `Content-Length: 1 2` to be interpreted as having a value of `12`. The HTTP specification does not allow for spaces in the `Content-Length` value and the Node.js HTTP parser has been brought into line on this particular difference. The security risk of this flaw to Node.js users is considered to be VERY LOW as it is difficult, and may be impossible, to craft an attack that makes use of this flaw in a way that could not already be achieved by supplying an incorrect value for `Content-Length`. Vulnerabilities may exist in user-code that make incorrect assumptions about the potential accuracy of this value compared to the actual length of the data supplied. Node.js users crafting lower-level HTTP utilities are advised to re-check the length of any input supplied after parsing is complete.

CVE-2018-7208	In the coff_pointerize_aux function in coffgen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, an index is not validated, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted file, as demonstrated by objcopy of a COFF object.
CVE-2018-7225	An issue was discovered in LibVNCServer through 0.9.11. rfbProcessClientNormalMessage() in rfbserver.c does not sanitize msg.cct.length, leading to access to uninitialized and potentially sensitive data or possibly unspecified other impact (e.g., an integer overflow) via specially crafted VNC packets.
CVE-2018-7409	In unixODBC before 2.3.5, there is a buffer overflow in the unicode_to_ansi_copy() function in DriverManager/_info.c.
CVE-2018-7418	In Wireshark 2.2.0 to 2.2.12 and 2.4.0 to 2.4.4, the SIGCOMP dissector could crash. This was addressed in epan/dissectors/packet-sigcomp.c by correcting the extraction of the length value.
CVE-2018-7456	A NULL Pointer Dereference occurs in the function TIFFPrintDirectory in tif_print.c in LibTIFF 3.9.3, 3.9.4, 3.9.5, 3.9.6, 3.9.7, 4.0.0alpha4, 4.0.0alpha5, 4.0.0alpha6, 4.0.0beta7, 4.0.0, 4.0.1, 4.0.2, 4.0.3, 4.0.4, 4.0.4beta, 4.0.5, 4.0.6, 4.0.7, 4.0.8 and 4.0.9 when using the tiffinfo tool to print crafted TIFF information, a different vulnerability than CVE-2017-18013. (This affects an earlier part of the TIFFPrintDirectory function that was not addressed by the CVE-2017-18013 patch.)
CVE-2018-7485	The SQLWriteFileDSN function in odbcinst/SQLWriteFileDSN.c in unixODBC 2.3.5 has strncpy arguments in the wrong order, which allows attackers to cause a denial of service or possibly have unspecified other impact.
CVE-2018-7548	In subst.c in zsh through 5.4.2, there is a NULL pointer dereference when using \${(PA)...} on an empty array result.
CVE-2018-7549	In params.c in zsh through 5.4.2, there is a crash during a copy of an empty hash table, as demonstrated by typeset -p.
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-2018-7568	The parse_die function in dwarf1.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (integer overflow and application

	crash) via an ELF file with corrupt dwarf1 debug information, as demonstrated by nm.
CVE-2018-7569	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (integer underflow or overflow, and application crash) via an ELF file with a corrupt DWARF FORM block, as demonstrated by nm.
CVE-2018-7643	The display_debug_ranges function in dwarf.c in GNU Binutils 2.30 allows remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact via a crafted ELF file, as demonstrated by objdump.
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-2018-7727	An issue was discovered in ZZIPlib 0.13.68. There is a memory leak triggered in the function zzip_mem_disk_new in memdisk.c, which will lead to a denial of service attack.
CVE-2018-7730	An issue was discovered in Exempi through 2.4.4. A certain case of a 0xffffffff length is mishandled in XMPFiles/source/FormatSupport/PSIR_FileWriter.cpp, leading to a heap-based buffer over-read in the PSD_MetaData::CacheFileData() function.
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-2018-7995	** DISPUTED ** Race condition in the store_int_with_restart() function in arch/x86/kernel/cpu/mcheck/mce.c in the Linux kernel through 4.15.7 allows local users to cause a denial of service (panic) by leveraging root access to write

	<p>to the check_interval file in a /sys/devices/system/machinecheck/machinecheck<cpu number> directory. NOTE: a third party has indicated that this report is not security relevant.</p>
CVE-2018-8007	<p>Apache CouchDB administrative users can configure the database server via HTTP(S). Due to insufficient validation of administrator-supplied configuration settings via the HTTP API, it is possible for a CouchDB administrator user to escalate their privileges to that of the operating system's user that CouchDB runs under, by bypassing the blacklist of configuration settings that are not allowed to be modified via the HTTP API. This privilege escalation effectively allows an existing CouchDB admin user to gain arbitrary remote code execution, bypassing already disclosed CVE-2017-12636. Mitigation: All users should upgrade to CouchDB releases 1.7.2 or 2.1.2.</p>
CVE-2018-8011	<p>By specially crafting HTTP requests, the mod_md challenge handler would dereference a NULL pointer and cause the child process to segfault. This could be used to DoS the server. Fixed in Apache HTTP Server 2.4.34 (Affected 2.4.33).</p>
CVE-2018-8014	<p>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.</p>
CVE-2018-8016	<p>The default configuration in Apache Cassandra 3.8 through 3.11.1 binds an unauthenticated JMX/RMI interface to all network interfaces, which allows remote attackers to execute arbitrary Java code via an RMI request. This issue is a regression of CVE-2015-0225. The regression was introduced in https://issues.apache.org/jira/browse/CASSANDRA-12109. The fix for the regression is implemented in https://issues.apache.org/jira/browse/CASSANDRA-14173. This fix is contained in the 3.11.2 release of Apache Cassandra.</p>
CVE-2018-8034	<p>The host name verification when using TLS with the WebSocket client was missing. It is now enabled by default. Versions Affected: Apache Tomcat 9.0.0.M1 to 9.0.9, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52, and 7.0.35 to 7.0.88.</p>
CVE-2018-8043	<p>The unimac_mdio_probe function in drivers/net/phy/mdio-bcm-unimac.c in the Linux kernel through 4.15.8 does not validate certain resource availability, which</p>

	allows local users to cause a denial of service (NULL pointer dereference).
CVE-2018-8088	org.slf4j.ext.EventData in the slf4j-ext module in QOS.CH SLF4J before 1.8.0-beta2 allows remote attackers to bypass intended access restrictions via crafted data. EventData in the slf4j-ext module in QOS.CH SLF4J, has been fixed in SLF4J versions 1.7.26 later and in the 2.0.x series.
CVE-2018-8777	In Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1, an attacker can pass a large HTTP request with a crafted header to WEBrick server or a crafted body to WEBrick server/handler and cause a denial of service (memory consumption).
CVE-2018-8778	In Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1, an attacker controlling the unpacking format (similar to format string vulnerabilities) can trigger a buffer under-read in the String#unpack method, resulting in a massive and controlled information disclosure.
CVE-2018-8779	In Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1, the UNIXServer.open and UNIXSocket.open methods are not checked for null characters. It may be connected to an unintended socket.
CVE-2018-8780	In Ruby before 2.2.10, 2.3.x before 2.3.7, 2.4.x before 2.4.4, 2.5.x before 2.5.1, and 2.6.0-preview1, the Dir.open, Dir.new, Dir.entries and Dir.empty? methods do not check NULL characters. When using the corresponding method, unintentional directory traversal may be performed.
CVE-2018-8786	FreeRDP prior to version 2.0.0-rc4 contains an Integer Truncation that leads to a Heap-Based Buffer Overflow in function update_read_bitmap_update() and results in a memory corruption and probably even a remote code execution.
CVE-2018-8787	FreeRDP prior to version 2.0.0-rc4 contains an Integer Overflow that leads to a Heap-Based Buffer Overflow in function gdi_Bitmap_Decompress() and results in a memory corruption and probably even a remote code execution.
CVE-2018-8788	FreeRDP prior to version 2.0.0-rc4 contains an Out-Of-Bounds Write of up to 4 bytes in function nsc_rle_decode() that results in a memory corruption and possibly even a remote code execution.
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-2018-8897	A statement in the System Programming Guide of the Intel 64 and IA-32 Architectures Software Developer's Manual (SDM) was mishandled in the development of some or all operating-system kernels, resulting in unexpected behavior for #DB exceptions that are deferred by MOV SS or POP SS, as demonstrated by (for example) privilege escalation in Windows, macOS, some Xen configurations, or FreeBSD, or a Linux kernel crash. The MOV to SS and POP SS instructions inhibit interrupts (including NMIs), data breakpoints, and single step trap exceptions until the instruction boundary following the next instruction (SDM Vol. 3A; section 6.8.3). (The inhibited data breakpoints are those on memory accessed by the MOV to SS or POP to SS instruction itself.) Note that debug exceptions are not inhibited by the interrupt enable (EFLAGS.IF) system flag (SDM Vol. 3A; section 2.3). If the instruction following the MOV to SS or POP to SS instruction is an instruction like SYSCALL, SYSENTER, INT 3, etc. that transfers control to the operating system at CPL < 3, the debug exception is delivered after the transfer to CPL < 3 is complete. OS kernels may not expect this order of events and may therefore experience unexpected behavior when it occurs.
CVE-2018-8905	In LibTIFF 4.0.9, a heap-based buffer overflow occurs in the function LZWDecodeCompat in tif_lzw.c via a crafted TIFF file, as demonstrated by tiff2ps.
CVE-2018-8976	In Exiv2 0.26, jpgimage.cpp allows remote attackers to cause a denial of service (image.cpp Exiv2::Internal::stringFormat out-of-bounds read) via a crafted file.
CVE-2018-8977	In Exiv2 0.26, the Exiv2::Internal::printCsLensFFFF function in canonmn_int.cpp allows remote attackers to cause a denial of service (invalid memory access) via a crafted file.
CVE-2018-9133	ImageMagick 7.0.7-26 Q16 has excessive iteration in the DecodeLablImage and EncodeLablImage 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-2018-9305	In Exiv2 0.26, an out-of-bounds read in IptcData::printStructure in iptc.c could result in a crash or information leak, related to the "== 0x1c" case.
CVE-2018-9363	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.

CVE-2018-9516	In hid_debug_events_read of drivers/hid/hid-debug.c, there is a possible out of bounds write due to a missing bounds check. 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-71361580.
CVE-2019-0160	Buffer overflow in system firmware for EDK II may allow unauthenticated user to potentially enable escalation of privilege and/or denial of service via network access.
CVE-2019-0161	Stack overflow in XHCI for EDK II may allow an unauthenticated user to potentially enable denial of service via local access.
CVE-2019-0193	In Apache Solr, the DataImportHandler, an optional but popular module to pull in data from databases and other sources, has a feature in which the whole DIH configuration can come from a request's "dataConfig" parameter. The debug mode of the DIH admin screen uses this to allow convenient debugging / development of a DIH config. Since a DIH config can contain scripts, this parameter is a security risk. Starting with version 8.2.0 of Solr, use of this parameter requires setting the Java System property "enable.dih.dataConfigParam" to true.
CVE-2019-0196	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
CVE-2019-0197	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
CVE-2019-0211	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
CVE-2019-0215	In Apache HTTP Server 2.4 releases 2.4.37 and 2.4.38, a bug in mod_ssl when using per-location client certificate verification with TLSv1.3 allowed a client to bypass configured access control restrictions.

CVE-2019-0217	In Apache HTTP Server 2.4 release 2.4.38 and prior, a race condition in mod_auth_digest when running in a threaded server could allow a user with valid credentials to authenticate using another username, bypassing configured access control restrictions.
CVE-2019-0220	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
CVE-2019-0816	A security feature bypass exists in Azure SSH Keypairs, due to a change in the provisioning logic for some Linux images that use cloud-init, aka 'Azure SSH Keypairs Security Feature Bypass Vulnerability'.
CVE-2019-1000019	libarchive version commit bf9aec176c6748f0ee7a678c5f9f9555b9a757c1 onwards (release v3.0.2 onwards) contains a CWE-125: Out-of-bounds Read vulnerability in 7zip decompression, archive_read_support_format_7zip.c, header_bytes() that can result in a crash (denial of service). This attack appears to be exploitable via the victim opening a specially crafted 7zip file.
CVE-2019-1000020	libarchive version commit 5a98dcf8a86364b3c2c469c85b93647dfb139961 onwards (version v2.8.0 onwards) contains a CWE-835: Loop with Unreachable Exit Condition ('Infinite Loop') vulnerability in ISO9660 parser, archive_read_support_format_iso9660.c, read_CE()/parse_rockridge() that can result in DoS by infinite loop. This attack appears to be exploitable via the victim opening a specially crafted ISO9660 file.
CVE-2019-1003003	An improper authorization vulnerability exists in Jenkins 2.158 and earlier, LTS 2.150.1 and earlier in core/src/main/java/hudson/security/TokenBasedRememberMeServices2.java that allows attackers with Overall/RunScripts permission to craft Remember Me cookies that would never expire, allowing e.g. to persist access to temporarily compromised user accounts.
CVE-2019-1003004	An improper authorization vulnerability exists in Jenkins 2.158 and earlier, LTS 2.150.1 and earlier in core/src/main/java/hudson/security/AuthenticationProcessingFilter2.java that allows attackers to extend the duration of active HTTP sessions indefinitely even though the user account may have been deleted in the mean time.
CVE-2019-1003049	Users who cached their CLI authentication before Jenkins was updated to 2.150.2 and newer, or 2.160

	and newer, would remain authenticated in Jenkins 2.171 and earlier and Jenkins LTS 2.164.1 and earlier, because the fix for CVE-2019-1003004 in these releases did not reject existing remoting-based CLI authentication caches.
CVE-2019-1003050	The f:validateButton form control for the Jenkins UI did not properly escape job URLs in Jenkins 2.171 and earlier and Jenkins LTS 2.164.1 and earlier, resulting in a cross-site scripting (XSS) vulnerability exploitable by users with the ability to control job names.
CVE-2019-10063	Flatpak before 1.0.8, 1.1.x and 1.2.x before 1.2.4, and 1.3.x before 1.3.1 allows a sandbox bypass. Flatpak versions since 0.8.1 address CVE-2017-5226 by using a seccomp filter to prevent sandboxed apps from using the TIOCSTI ioctl, which could otherwise be used to inject commands into the controlling terminal so that they would be executed outside the sandbox after the sandboxed app exits. This fix was incomplete: on 64-bit platforms, the seccomp filter could be bypassed by an ioctl request number that has TIOCSTI in its 32 least significant bits and an arbitrary nonzero value in its 32 most significant bits, which the Linux kernel would treat as equivalent to TIOCSTI.
CVE-2019-10086	In Apache Commons Beanutils 1.9.2, a special BeanInspector class was added which allows suppressing the ability for an attacker to access the classloader via the class property available on all Java objects. We, however were not using this by default characteristic of the PropertyUtilsBean.
CVE-2019-10092	In Apache HTTP Server 2.4.0-2.4.39, a limited cross-site scripting issue was reported affecting the mod_proxy error page. An attacker could cause the link on the error page to be malformed and instead point to a page of their choice. This would only be exploitable where a server was set up with proxying enabled but was misconfigured in such a way that the Proxy Error page was displayed.
CVE-2019-10097	In Apache HTTP Server 2.4.32-2.4.39, when mod_remoteip was configured to use a trusted intermediary proxy server using the "PROXY" protocol, a specially crafted PROXY header could trigger a stack buffer overflow or NULL pointer deference. This vulnerability could only be triggered by a trusted proxy and not by untrusted HTTP clients.
CVE-2019-10098	In Apache HTTP server 2.4.0 to 2.4.39, Redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.
CVE-2019-1010305	libmspack 0.9.1alpha is affected by: Buffer Overflow. The impact is: Information Disclosure.

	The component is: function chmd_read_headers() in libmspack(file libmspack/mspack/chmd.c). The attack vector is: the victim must open a specially crafted chm file. The fixed version is: after commit 2f084136cfe0d05e5bf5703f3e83c6d955234b4d.
CVE-2019-10131	An off-by-one read vulnerability was discovered in ImageMagick before version 7.0.7-28 in the formatIPTCfromBuffer function in coders/meta.c. A local attacker may use this flaw to read beyond the end of the buffer or to crash the program.
CVE-2019-10132	A vulnerability was found in libvirt >= 4.1.0 in the virtlockd-admin.socket and virtlogd-admin.socket systemd units. A missing SocketMode configuration parameter allows any user on the host to connect using virtlockd-admin-sock or virtlogd-admin-sock and perform administrative tasks against the virtlockd and virtlogd daemons.
CVE-2019-10142	A flaw was found in the Linux kernel's freescale hypervisor manager implementation, kernel versions 5.0.x up to, excluding 5.0.17. A parameter passed to an ioctl was incorrectly validated and used in size calculations for the page size calculation. An attacker can use this flaw to crash the system, corrupt memory, or create other adverse security affects.
CVE-2019-10143	** DISPUTED ** It was discovered freeradius up to and including version 3.0.19 does not correctly configure logrotate, allowing a local attacker who already has control of the radiusd user to escalate his privileges to root, by tricking logrotate into writing a radiusd-writable file to a directory normally inaccessible by the radiusd user. NOTE: the upstream software maintainer has stated "there is simply no way for anyone to gain privileges through this alleged issue."
CVE-2019-10146	A Reflected Cross Site Scripting flaw was found in all pki-core 10.x.x versions module from the pki-core server due to the CA Agent Service not properly sanitizing the certificate request page. An attacker could inject a specially crafted value that will be executed on the victim's browser.
CVE-2019-10153	A flaw was discovered in fence-agents, prior to version 4.3.4, where using non-ASCII characters in a guest VM's comment or other fields would cause fence_rhevm to exit with an exception. In cluster environments, this could lead to preventing automated recovery or otherwise denying service to clusters of which that VM is a member.
CVE-2019-10160	A security regression of CVE-2019-9636 was discovered in python since commit d537ab0ff9767ef024f26246899728f0116b1ec3 affecting versions 2.7, 3.5, 3.6, 3.7 and from v3.8.0a4 through v3.8.0b1, which still allows an attacker to

	exploit CVE-2019-9636 by abusing the user and password parts of a URL. When an application parses user-supplied URLs to store cookies, authentication credentials, or other kind of information, it is possible for an attacker to provide specially crafted URLs to make the application locate host-related information (e.g. cookies, authentication data) and send them to a different host than where it should, unlike if the URLs had been correctly parsed. The result of an attack may vary based on the application.
CVE-2019-10161	It was discovered that libvirtd before versions 4.10.1 and 5.4.1 would permit read-only clients to use the virDomainSaveImageGetXMLDesc() API, specifying an arbitrary path which would be accessed with the permissions of the libvirtd process. An attacker with access to the libvirtd socket could use this to probe the existence of arbitrary files, cause denial of service or cause libvirtd to execute arbitrary programs.
CVE-2019-10166	It was discovered that libvirtd, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, would permit readonly clients to use the virDomainManagedSaveDefineXML() API, which would permit them to modify managed save state files. If a managed save had already been created by a privileged user, a local attacker could modify this file such that libvirtd would execute an arbitrary program when the domain was resumed.
CVE-2019-10167	The virConnectGetDomainCapabilities() libvirt API, versions 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accepts an "emulatorbin" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges.
CVE-2019-10168	The virConnectBaselineHypervisorCPU() and virConnectCompareHypervisorCPU() libvirt APIs, 4.x.x before 4.10.1 and 5.x.x before 5.4.1, accept an "emulator" argument to specify the program providing emulation for a domain. Since v1.2.19, libvirt will execute that program to probe the domain's capabilities. Read-only clients could specify an arbitrary path for this argument, causing libvirtd to execute a crafted executable with its own privileges.
CVE-2019-10179	A vulnerability was found in all pki-core 10.x.x versions, where the Key Recovery Authority (KRA) Agent Service did not properly sanitize recovery request search page, enabling a Reflected Cross Site Scripting (XSS) vulnerability. An attacker could trick an authenticated victim into executing specially crafted Javascript code.
CVE-2019-10195	A flaw was found in IPA, all 4.6.x versions before 4.6.7, all 4.7.x versions before 4.7.4 and all 4.8.x

	versions before 4.8.3, in the way that FreeIPA's batch processing API logged operations. This included passing user passwords in clear text on FreeIPA masters. Batch processing of commands with passwords as arguments or options is not performed by default in FreeIPA but is possible by third-party components. An attacker having access to system logs on FreeIPA masters could use this flaw to produce log file content with passwords exposed.
CVE-2019-10197	A flaw was found in samba versions 4.9.x up to 4.9.13, samba 4.10.x up to 4.10.8 and samba 4.11.x up to 4.11.0rc3, when certain parameters were set in the samba configuration file. An unauthenticated attacker could use this flaw to escape the shared directory and access the contents of directories outside the share.
CVE-2019-10208	A flaw was discovered in postgresql versions 9.4.x before 9.4.24, 9.5.x before 9.5.19, 9.6.x before 9.6.15, 10.x before 10.10 and 11.x before 11.5 where arbitrary SQL statements can be executed given a suitable SECURITY DEFINER function. An attacker, with EXECUTE permission on the function, can execute arbitrary SQL as the owner of the function.
CVE-2019-10218	A flaw was found in the samba client, all samba versions before samba 4.11.2, 4.10.10 and 4.9.15, where a malicious server can supply a pathname to the client with separators. This could allow the client to access files and folders outside of the SMB network pathnames. An attacker could use this vulnerability to create files outside of the current working directory using the privileges of the client user.
CVE-2019-10221	A Reflected Cross Site Scripting vulnerability was found in all pki-core 10.x.x versions, where the pki-ca module from the pki-core server. This flaw is caused by missing sanitization of the GET URL parameters. An attacker could abuse this flaw to trick an authenticated user into clicking a specially crafted link which can execute arbitrary code when viewed in a browser.
CVE-2019-10352	A path traversal vulnerability in Jenkins 2.185 and earlier, LTS 2.176.1 and earlier in core/src/main/java/hudson/model/FileParameterValue.java allowed attackers with Job/Configure permission to define a file parameter with a file name outside the intended directory, resulting in an arbitrary file write on the Jenkins master when scheduling a build.
CVE-2019-10353	CSRF tokens in Jenkins 2.185 and earlier, LTS 2.176.1 and earlier did not expire, thereby allowing attackers able to obtain them to bypass CSRF protection.
CVE-2019-10354	A vulnerability in the Stapler web framework used in Jenkins 2.185 and earlier, LTS 2.176.1 and earlier allowed attackers to access view fragments directly,

	bypassing permission checks and possibly obtain sensitive information.
CVE-2019-10383	A stored cross-site scripting vulnerability in Jenkins 2.191 and earlier, LTS 2.176.2 and earlier allowed attackers with Overall/Administer permission to configure the update site URL to inject arbitrary HTML and JavaScript in update center web pages.
CVE-2019-10384	Jenkins 2.191 and earlier, LTS 2.176.2 and earlier allowed users to obtain CSRF tokens without an associated web session ID, resulting in CSRF tokens that did not expire and could be used to bypass CSRF protection for the anonymous user.
CVE-2019-10401	In Jenkins 2.196 and earlier, LTS 2.176.3 and earlier, the f:expandableTextBox form control interpreted its content as HTML when expanded, resulting in a stored XSS vulnerability exploitable by users with permission to define its contents (typically Job/Configure).
CVE-2019-10402	In Jenkins 2.196 and earlier, LTS 2.176.3 and earlier, the f:combobox form control interpreted its item labels as HTML, resulting in a stored XSS vulnerability exploitable by users with permission to define its contents.
CVE-2019-10403	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier did not escape the SCM tag name on the tooltip for SCM tag actions, resulting in a stored XSS vulnerability exploitable by users able to control SCM tag names for these actions.
CVE-2019-10404	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier did not escape the reason why a queue items is blocked in tooltips, resulting in a stored XSS vulnerability exploitable by users able to control parts of the reason a queue item is blocked, such as label expressions not matching any idle executors.
CVE-2019-10405	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier printed the value of the "Cookie" HTTP request header on the /whoAmI/ URL, allowing attackers exploiting another XSS vulnerability to obtain the HTTP session cookie despite it being marked HttpOnly.
CVE-2019-10406	Jenkins 2.196 and earlier, LTS 2.176.3 and earlier did not restrict or filter values set as Jenkins URL in the global configuration, resulting in a stored XSS vulnerability exploitable by attackers with Overall/ Administer permission.
CVE-2019-10650	In ImageMagick 7.0.8-36 Q16, there is a heap-based buffer over-read in the function WriteTIFFImage of coders/tiff.c, which allows an attacker to cause a denial of service or information disclosure via a crafted image file.

CVE-2019-10871	An issue was discovered in Poppler 0.74.0. There is a heap-based buffer over-read in the function PSOutputDev::checkPageSlice at PSOutputDev.cc.
CVE-2019-11043	In PHP versions 7.1.x below 7.1.33, 7.2.x below 7.2.24 and 7.3.x below 7.3.11 in certain configurations of FPM setup it is possible to cause FPM module to write past allocated buffers into the space reserved for CGI protocol data, thus opening the possibility of remote code execution.
CVE-2019-11068	libxslt through 1.1.33 allows bypass of a protection mechanism because callers of xsltCheckRead and xsltCheckWrite permit access even upon receiving a -1 error code. xsltCheckRead can return -1 for a crafted URL that is not actually invalid and is subsequently loaded.
CVE-2019-11070	WebKitGTK and WPE WebKit prior to version 2.24.1 failed to properly apply configured HTTP proxy settings when downloading livestream video (HLS, DASH, or Smooth Streaming), an error resulting in deanonymization. This issue was corrected by changing the way livestreams are downloaded.
CVE-2019-11091	Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf
CVE-2019-11135	TSX Asynchronous Abort condition on some CPUs utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.
CVE-2019-11139	Improper conditions check in the voltage modulation interface for some Intel(R) Xeon(R) Scalable Processors may allow a privileged user to potentially enable denial of service via local access.
CVE-2019-11234	FreeRADIUS before 3.0.19 does not prevent use of reflection for authentication spoofing, aka a "Dragonblood" issue, a similar issue to CVE-2019-9497.
CVE-2019-11235	FreeRADIUS before 3.0.19 mishandles the "each participant verifies that the received scalar is within a range, and that the received group element is a valid point on the curve being used" protection mechanism, aka a "Dragonblood" issue, a similar issue to CVE-2019-9498 and CVE-2019-9499.

CVE-2019-11236	In the urllib3 library through 1.24.1 for Python, CRLF injection is possible if the attacker controls the request parameter.
CVE-2019-1125	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073.
CVE-2019-11251	The Kubernetes kubectl cp command in versions 1.1-1.12, and versions prior to 1.13.11, 1.14.7, and 1.15.4 allows a combination of two symlinks provided by tar output of a malicious container to place a file outside of the destination directory specified in the kubectl cp invocation. This could be used to allow an attacker to place a nefarious file using a symlink, outside of the destination tree.
CVE-2019-11253	Improper input validation in the Kubernetes API server in versions v1.0-1.12 and versions prior to v1.13.12, v1.14.8, v1.15.5, and v1.16.2 allows authorized users to send malicious YAML or JSON payloads, causing the API server to consume excessive CPU or memory, potentially crashing and becoming unavailable. Prior to v1.14.0, default RBAC policy authorized anonymous users to submit requests that could trigger this vulnerability. Clusters upgraded from a version prior to v1.14.0 keep the more permissive policy by default for backwards compatibility.
CVE-2019-11324	The urllib3 library before 1.24.2 for Python mishandles certain cases where the desired set of CA certificates is different from the OS store of CA certificates, which results in SSL connections succeeding in situations where a verification failure is the correct outcome. This is related to use of the ssl_context, ca_certs, or ca_certs_dir argument.
CVE-2019-11358	jQuery before 3.4.0, as used in Drupal, Backdrop CMS, and other products, mishandles jQuery.extend(true, {}, ...) because of Object.prototype pollution. If an unsanitized source object contained an enumerable __proto__ property, it could extend the native Object.prototype.
CVE-2019-11459	The tiff_document_render() and tiff_document_get_thumbnail() functions in the TIFF document backend in GNOME Evince through 3.32.0 did not handle errors from TIFFReadRGBALImageOriented(), leading to uninitialized memory use when processing certain TIFF image files.
CVE-2019-11470	The cineon parsing component in ImageMagick 7.0.8-26 Q16 allows attackers to cause a denial-of-service (uncontrolled resource consumption) by crafting

	a Cineon image with an incorrect claimed image size. This occurs because ReadCINImage in coders/cin.c lacks a check for insufficient image data in a file.
CVE-2019-11472	ReadXWDImage in coders/xwd.c in the XWD image parsing component of ImageMagick 7.0.8-41 Q16 allows attackers to cause a denial-of-service (divide-by-zero error) by crafting an XWD image file in which the header indicates neither LSB first nor MSB first.
CVE-2019-11477	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff.
CVE-2019-11478	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e.
CVE-2019-11479	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363.
CVE-2019-11500	In Dovecot before 2.2.36.4 and 2.3.x before 2.3.7.2 (and Pigeonhole before 0.5.7.2), protocol processing can fail for quoted strings. This occurs because '\0' characters are mishandled, and can lead to out-of-bounds writes and remote code execution.
CVE-2019-11581	There was a server-side template injection vulnerability in Jira Server and Data Center, in the ContactAdministrators and the SendBulkMail actions. An attacker is able to remotely execute code on systems that run a vulnerable version of Jira Server or Data Center. All versions of Jira Server and Data Center from 4.4.0 before 7.6.14, from 7.7.0 before 7.13.5, from 8.0.0 before 8.0.3, from 8.1.0 before 8.1.2, and from 8.2.0 before 8.2.3 are affected by this vulnerability.

CVE-2019-11597	In ImageMagick 7.0.8-43 Q16, there is a heap-based buffer over-read in the function WriteTIFFImage of coders/tiff.c, which allows an attacker to cause a denial of service or possibly information disclosure via a crafted image file.
CVE-2019-11598	In ImageMagick 7.0.8-40 Q16, there is a heap-based buffer over-read in the function WritePNMImage of coders/pnm.c, which allows an attacker to cause a denial of service or possibly information disclosure via a crafted image file. This is related to SetGrayscaleImage in MagickCore/quantize.c.
CVE-2019-11599	The coredump implementation in the Linux kernel before 5.0.10 does not use locking or other mechanisms to prevent vma layout or vma flags changes while it runs, which allows local users to obtain sensitive information, cause a denial of service, or possibly have unspecified other impact by triggering a race condition with mmget_not_zero or get_task_mm calls. This is related to fs/userfaultfd.c, mm/mmap.c, fs/proc/task_mmu.c, and drivers/infiniband/core/uverbs_main.c.
CVE-2019-11691	A use-after-free vulnerability can occur when working with XMLHttpRequest (XHR) in an event loop, causing the XHR main thread to be called after it has been freed. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.
CVE-2019-11692	A use-after-free vulnerability can occur when listeners are removed from the event listener manager while still in use, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.
CVE-2019-11693	The bufferdata function in WebGL is vulnerable to a buffer overflow with specific graphics drivers on Linux. This could result in malicious content freezing a tab or triggering a potentially exploitable crash. *Note: this issue only occurs on Linux. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.
CVE-2019-11698	If a crafted hyperlink is dragged and dropped to the bookmark bar or sidebar and the resulting bookmark is subsequently dragged and dropped into the web content area, an arbitrary query of a user's browser history can be run and transmitted to the content page via drop event data. This allows for the theft of browser history by a malicious site. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.
CVE-2019-11703	A flaw in Thunderbird's implementation of iCal causes a heap buffer overflow in parser_get_next_char when

	processing certain email messages, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7.1.
CVE-2019-11704	A flaw in Thunderbird's implementation of iCal causes a heap buffer overflow in <code>icalmemory_strdup_and_dequote</code> when processing certain email messages, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7.1.
CVE-2019-11705	A flaw in Thunderbird's implementation of iCal causes a stack buffer overflow in <code>icalrecur_add_bydayrules</code> when processing certain email messages, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7.1.
CVE-2019-11706	A flaw in Thunderbird's implementation of iCal causes a type confusion in <code>icaltimezone_get_vtimezone_properties</code> when processing certain email messages, resulting in a crash. This vulnerability affects Thunderbird < 60.7.1.
CVE-2019-11707	A type confusion vulnerability can occur when manipulating JavaScript objects due to issues in <code>Array.pop</code> . This can allow for an exploitable crash. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Firefox ESR < 60.7.1, Firefox < 67.0.3, and Thunderbird < 60.7.2.
CVE-2019-11708	Insufficient vetting of parameters passed with the <code>Prompt:Open</code> IPC message between child and parent processes can result in the non-sandboxed parent process opening web content chosen by a compromised child process. When combined with additional vulnerabilities this could result in executing arbitrary code on the user's computer. This vulnerability affects Firefox ESR < 60.7.2, Firefox < 67.0.4, and Thunderbird < 60.7.2.
CVE-2019-11709	Mozilla developers and community members reported memory safety bugs present in Firefox 67 and Firefox ESR 60.7. 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 Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.
CVE-2019-11711	When an inner window is reused, it does not consider the use of <code>document.domain</code> for cross-origin protections. If pages on different subdomains ever cooperatively use <code>document.domain</code> , then either page can abuse this to inject script into arbitrary pages on the other subdomain, even those that did not use <code>document.domain</code> to relax their origin security. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.

CVE-2019-11713	A use-after-free vulnerability can occur in HTTP/2 when a cached HTTP/2 stream is closed while still in use, resulting in a potentially exploitable crash. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.
CVE-2019-11715	Due to an error while parsing page content, it is possible for properly sanitized user input to be misinterpreted and lead to XSS hazards on web sites in certain circumstances. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.
CVE-2019-11717	A vulnerability exists where the caret ("^") character is improperly escaped constructing some URLs due to it being used as a separator, allowing for possible spoofing of origin attributes. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.
CVE-2019-11719	When importing a curve25519 private key in PKCS#8format with leading 0x00 bytes, it is possible to trigger an out-of-bounds read in the Network Security Services (NSS) library. This could lead to information disclosure. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.
CVE-2019-11727	A vulnerability exists where it possible to force Network Security Services (NSS) to sign CertificateVerify with PKCS#1 v1.5 signatures when those are the only ones advertised by server in CertificateRequest in TLS 1.3. PKCS#1 v1.5 signatures should not be used for TLS 1.3 messages. This vulnerability affects Firefox < 68.
CVE-2019-11729	Empty or malformed p256-ECDH public keys may trigger a segmentation fault due values being improperly sanitized before being copied into memory and used. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.
CVE-2019-11730	A vulnerability exists where if a user opens a locally saved HTML file, this file can use file: URLs to access other files in the same directory or sub-directories if the names are known or guessed. The Fetch API can then be used to read the contents of any files stored in these directories and they may uploaded to a server. It was demonstrated that in combination with a popular Android messaging app, if a malicious HTML attachment is sent to a user and they opened that attachment in Firefox, due to that app's predictable pattern for locally-saved file names, it is possible to read attachments the victim received from other correspondents. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.
CVE-2019-11739	Encrypted S/MIME parts in a crafted multipart/alternative message can leak plaintext when included

	in a a HTML reply/forward. This vulnerability affects Thunderbird < 68.1 and Thunderbird < 60.9.
CVE-2019-11740	Mozilla developers and community members reported memory safety bugs present in Firefox 68, Firefox ESR 68, and Firefox 60.8. 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 Firefox < 69, Thunderbird < 68.1, Thunderbird < 60.9, Firefox ESR < 60.9, and Firefox ESR < 68.1.
CVE-2019-11742	A same-origin policy violation occurs allowing the theft of cross-origin images through a combination of SVG filters and a <canvas> element due to an error in how same-origin policy is applied to cached image content. The resulting same-origin policy violation could allow for data theft. This vulnerability affects Firefox < 69, Thunderbird < 68.1, Thunderbird < 60.9, Firefox ESR < 60.9, and Firefox ESR < 68.1.
CVE-2019-11743	Navigation events were not fully adhering to the W3C's "Navigation-Timing Level 2" draft specification in some instances for the unload event, which restricts access to detailed timing attributes to only be same-origin. This resulted in potential cross-origin information exposure of history through timing side-channel attacks. This vulnerability affects Firefox < 69, Thunderbird < 68.1, Thunderbird < 60.9, Firefox ESR < 60.9, and Firefox ESR < 68.1.
CVE-2019-11744	Some HTML elements, such as <title> and <textarea>, can contain literal angle brackets without treating them as markup. It is possible to pass a literal closing tag to .innerHTML on these elements, and subsequent content after that will be parsed as if it were outside the tag. This can lead to XSS if a site does not filter user input as strictly for these elements as it does for other elements. This vulnerability affects Firefox < 69, Thunderbird < 68.1, Thunderbird < 60.9, Firefox ESR < 60.9, and Firefox ESR < 68.1.
CVE-2019-11745	When encrypting with a block cipher, if a call to NSC_EncryptUpdate was made with data smaller than the block size, a small out of bounds write could occur. This could have caused heap corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.3, Firefox ESR < 68.3, and Firefox < 71.
CVE-2019-11746	A use-after-free vulnerability can occur while manipulating video elements if the body is freed while still in use. This results in a potentially exploitable crash. This vulnerability affects Firefox < 69, Thunderbird < 68.1, Thunderbird < 60.9, Firefox ESR < 60.9, and Firefox ESR < 68.1.

CVE-2019-11752	It is possible to delete an IndexedDB key value and subsequently try to extract it during conversion. This results in a use-after-free and a potentially exploitable crash. This vulnerability affects Firefox < 69, Thunderbird < 68.1, Thunderbird < 60.9, Firefox ESR < 60.9, and Firefox ESR < 68.1.
CVE-2019-11756	Improper refcounting of soft token session objects could cause a use-after-free and crash (likely limited to a denial of service). This vulnerability affects Firefox < 71.
CVE-2019-11757	When following the value's prototype chain, it was possible to retain a reference to a locale, delete it, and subsequently reference it. This resulted in a use-after-free and a potentially exploitable crash. This vulnerability affects Firefox < 70, Thunderbird < 68.2, and Firefox ESR < 68.2.
CVE-2019-11758	Mozilla community member Philipp reported a memory safety bug present in Firefox 68 when 360 Total Security was installed. This bug showed evidence of memory corruption in the accessibility engine and we presume that with enough effort that it could be exploited to run arbitrary code. This vulnerability affects Firefox < 69, Thunderbird < 68.2, and Firefox ESR < 68.2.
CVE-2019-11759	An attacker could have caused 4 bytes of HMAC output to be written past the end of a buffer stored on the stack. This could be used by an attacker to execute arbitrary code or more likely lead to a crash. This vulnerability affects Firefox < 70, Thunderbird < 68.2, and Firefox ESR < 68.2.
CVE-2019-11760	A fixed-size stack buffer could overflow in nrappkit when doing WebRTC signaling. This resulted in a potentially exploitable crash in some instances. This vulnerability affects Firefox < 70, Thunderbird < 68.2, and Firefox ESR < 68.2.
CVE-2019-11761	By using a form with a data URI it was possible to gain access to the privileged JSONView object that had been cloned into content. Impact from exposing this object appears to be minimal, however it was a bypass of existing defense in depth mechanisms. This vulnerability affects Firefox < 70, Thunderbird < 68.2, and Firefox ESR < 68.2.
CVE-2019-11762	If two same-origin documents set document.domain differently to become cross-origin, it was possible for them to call arbitrary DOM methods/getters/setters on the now-cross-origin window. This vulnerability affects Firefox < 70, Thunderbird < 68.2, and Firefox ESR < 68.2.
CVE-2019-11763	Failure to correctly handle null bytes when processing HTML entities resulted in Firefox incorrectly parsing these entities. This could have led to HTML comment

	text being treated as HTML which could have led to XSS in a web application under certain conditions. It could have also led to HTML entities being masked from filters - enabling the use of entities to mask the actual characters of interest from filters. This vulnerability affects Firefox < 70, Thunderbird < 68.2, and Firefox ESR < 68.2.
CVE-2019-11764	Mozilla developers and community members reported memory safety bugs present in Firefox 69 and Firefox ESR 68.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 70, Thunderbird < 68.2, and Firefox ESR < 68.2.
CVE-2019-11815	An issue was discovered in rds_tcp_kill_sock in net/rds/tcp.c in the Linux kernel before 5.0.8. There is a race condition leading to a use-after-free, related to net namespace cleanup.
CVE-2019-11833	fs/ext4/extents.c in the Linux kernel through 5.1.2 does not zero out the unused memory region in the extent tree block, which might allow local users to obtain sensitive information by reading uninitialized data in the filesystem.
CVE-2019-11884	The do_hidp_sock_ioctl function in net/bluetooth/hidp/sock.c in the Linux kernel before 5.0.15 allows a local user to obtain potentially sensitive information from kernel stack memory via a HIDPCONNADD command, because a name field may not end with a '\0' character.
CVE-2019-12155	interface_release_resource in hw/display/qxl.c in QEMU 3.1.x through 4.0.0 has a NULL pointer dereference.
CVE-2019-12222	An issue was discovered in libSDL2.a in Simple DirectMedia Layer (SDL) 2.0.9. There is an out-of-bounds read in the function SDL_InvalidateMap at video/SDL_pixels.c.
CVE-2019-12290	GNU libidn2 before 2.2.0 fails to perform the roundtrip checks specified in RFC3490 Section 4.2 when converting A-labels to U-labels. This makes it possible in some circumstances for one domain to impersonate another. By creating a malicious domain that matches a target domain except for the inclusion of certain punycoded Unicode characters (that would be discarded when converted first to a Unicode label and then back to an ASCII label), arbitrary domains can be impersonated.
CVE-2019-12293	In Poppler through 0.76.1, there is a heap-based buffer over-read in JPXStream::init in JPEG2000Stream.cc via data with inconsistent heights or widths.
CVE-2019-12420	In Apache SpamAssassin before 3.4.3, a message can be crafted in a way to use excessive resources.

	Upgrading to SA 3.4.3 as soon as possible is the recommended fix but details will not be shared publicly.
CVE-2019-12450	file_copy_fallback in gio/gfile.c in GNOME GLib 2.15.0 through 2.61.1 does not properly restrict file permissions while a copy operation is in progress. Instead, default permissions are used.
CVE-2019-12519	An issue was discovered in Squid through 4.7. When handling the tag <code>esi:when</code> when ESI is enabled, Squid calls <code>ESIExpression::Evaluate</code> . This function uses a fixed stack buffer to hold the expression while it's being evaluated. When processing the expression, it could either evaluate the top of the stack, or add a new member to the stack. When adding a new member, there is no check to ensure that the stack won't overflow.
CVE-2019-12525	An issue was discovered in Squid 3.3.9 through 3.5.28 and 4.x through 4.7. When Squid is configured to use Digest authentication, it parses the header <code>Proxy-Authorization</code> . It searches for certain tokens such as domain, uri, and qop. Squid checks if this token's value starts with a quote and ends with one. If so, it performs a <code>memcpy</code> of its length minus 2. Squid never checks whether the value is just a single quote (which would satisfy its requirements), leading to a <code>memcpy</code> of its length minus 1.
CVE-2019-12528	An issue was discovered in Squid before 4.10. It allows a crafted FTP server to trigger disclosure of sensitive information from heap memory, such as information associated with other users' sessions or non-Squid processes.
CVE-2019-12735	<code>getchar.c</code> in Vim before 8.1.1365 and Neovim before 0.3.6 allows remote attackers to execute arbitrary OS commands via the <code>:source!</code> command in a modeline, as demonstrated by <code>execute</code> in Vim, and <code>assert_fails</code> or <code>nvim_input</code> in Neovim.
CVE-2019-12779	<code>libqb</code> before 1.0.5 allows local users to overwrite arbitrary files via a symlink attack, because it uses predictable filenames (under <code>/dev/shm</code> and <code>/tmp</code>) without <code>O_EXCL</code> .
CVE-2019-12815	An arbitrary file copy vulnerability in <code>mod_copy</code> in ProFTPD up to 1.3.5b allows for remote code execution and information disclosure without authentication, a related issue to CVE-2015-3306.
CVE-2019-12900	<code>BZ2_decompress</code> in <code>decompress.c</code> in bzip2 through 1.0.6 has an out-of-bounds write when there are many selectors.
CVE-2019-12973	In OpenJPEG 2.3.1, there is excessive iteration in the <code>ojp_t1_encode_cblk</code> s function of <code>openjp2/t1.c</code> . Remote attackers could leverage this vulnerability to cause a

	denial of service via a crafted bmp file. This issue is similar to CVE-2018-6616.
CVE-2019-12974	A NULL pointer dereference in the function ReadPANGOImage in coders/pango.c and the function ReadVIDImage in coders/vid.c in ImageMagick 7.0.8-34 allows remote attackers to cause a denial of service via a crafted image.
CVE-2019-12975	ImageMagick 7.0.8-34 has a memory leak vulnerability in the WriteDPXImage function in coders/dpx.c.
CVE-2019-12976	ImageMagick 7.0.8-34 has a memory leak in the ReadPCLImage function in coders/pcl.c.
CVE-2019-12978	ImageMagick 7.0.8-34 has a "use of uninitialized value" vulnerability in the ReadPANGOImage function in coders/pango.c.
CVE-2019-12979	ImageMagick 7.0.8-34 has a "use of uninitialized value" vulnerability in the SyncImageSettings function in MagickCore/image.c. This is related to AcquireImage in magick/image.c.
CVE-2019-13038	mod_auth_mellon through 0.14.2 has an Open Redirect via the login?ReturnTo= substring, as demonstrated by omitting the // after http: in the target URL.
CVE-2019-13117	In numbers.c in libxslt 1.1.33, an xs: number with certain format strings could lead to a uninitialized read in xsltNumberFormatInsertNumbers. This could allow an attacker to discern whether a byte on the stack contains the characters A, a, I, i, or 0, or any other character.
CVE-2019-13118	In numbers.c in libxslt 1.1.33, a type holding grouping characters of an xs: number instruction was too narrow and an invalid character/length combination could be passed to xsltNumberFormatDecimal, leading to a read of uninitialized stack data.
CVE-2019-13133	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadBMPIImage in coders/bmp.c.
CVE-2019-13134	ImageMagick before 7.0.8-50 has a memory leak vulnerability in the function ReadVIFFImage in coders/viff.c.
CVE-2019-13135	ImageMagick before 7.0.8-50 has a "use of uninitialized value" vulnerability in the function ReadCUTImage in coders/cut.c.
CVE-2019-13139	In Docker before 18.09.4, an attacker who is capable of supplying or manipulating the build path for the "docker build" command would be able to gain command execution. An issue exists in the way "docker build" processes remote git URLs, and results in command injection into the underlying "git clone" command, leading to code execution in the context of the user.

	executing the "docker build" command. This occurs because git ref can be misinterpreted as a flag.
CVE-2019-13224	A use-after-free in onig_new_deluxe() in regext.c in Oniguruma 6.9.2 allows attackers to potentially cause information disclosure, denial of service, or possibly code execution by providing a crafted regular expression. The attacker provides a pair of a regex pattern and a string, with a multi-byte encoding that gets handled by onig_new_deluxe(). Oniguruma issues often affect Ruby, as well as common optional libraries for PHP and Rust.
CVE-2019-13225	A NULL Pointer Dereference in match_at() in regexec.c in Oniguruma 6.9.2 allows attackers to potentially cause denial of service by providing a crafted regular expression. Oniguruma issues often affect Ruby, as well as common optional libraries for PHP and Rust.
CVE-2019-13232	Info-ZIP UnZip 6.0 mishandles the overlapping of files inside a ZIP container, leading to denial of service (resource consumption), aka a "better zip bomb" issue.
CVE-2019-13295	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/threshold.c in AdaptiveThresholdImage because a width of zero is mishandled.
CVE-2019-13297	ImageMagick 7.0.8-50 Q16 has a heap-based buffer over-read at MagickCore/threshold.c in AdaptiveThresholdImage because a height of zero is mishandled.
CVE-2019-13300	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/statistic.c in EvaluateImages because of mishandling columns.
CVE-2019-13301	ImageMagick 7.0.8-50 Q16 has memory leaks in AcquireMagickMemory because of an AnnotateImage error.
CVE-2019-13304	ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of a misplaced assignment.
CVE-2019-13305	ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of a misplaced strncpy and an off-by-one error.
CVE-2019-13306	ImageMagick 7.0.8-50 Q16 has a stack-based buffer overflow at coders/pnm.c in WritePNMImage because of off-by-one errors.
CVE-2019-13307	ImageMagick 7.0.8-50 Q16 has a heap-based buffer overflow at MagickCore/statistic.c in EvaluateImages because of mishandling rows.
CVE-2019-13309	ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of mishandling the NoSuchImage error in CLIListOperatorImages in MagickWand/operation.c.

CVE-2019-13310	ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of an error in MagickWand/mogrify.c.
CVE-2019-13311	ImageMagick 7.0.8-50 Q16 has memory leaks at AcquireMagickMemory because of a wand/mogrify.c error.
CVE-2019-13313	libosinfo 1.5.0 allows local users to discover credentials by listing a process, because credentials are passed to osinfo-install-script via the command line.
CVE-2019-13345	The cachemgr.cgi web module of Squid through 4.7 has XSS via the user_name or auth parameter.
CVE-2019-13454	ImageMagick 7.0.8-54 Q16 allows Division by Zero in RemoveDuplicateLayers in MagickCore/layer.c.
CVE-2019-13456	In FreeRADIUS 3.0 through 3.0.19, on average 1 in every 2048 EAP-pwd handshakes fails because the password element cannot be found within 10 iterations of the hunting and pecking loop. This leaks information that an attacker can use to recover the password of any user. This information leakage is similar to the "Dragonblood" attack and CVE-2019-9494.
CVE-2019-1348	An issue was found in Git before v2.24.1, v2.23.1, v2.22.2, v2.21.1, v2.20.2, v2.19.3, v2.18.2, v2.17.3, v2.16.6, v2.15.4, and v2.14.6. The --export-marks option of git fast-import is exposed also via the in-stream command feature export-marks=... and it allows overwriting arbitrary paths.
CVE-2019-1349	A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input, aka 'Git for Visual Studio Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1350, CVE-2019-1352, CVE-2019-1354, CVE-2019-1387.
CVE-2019-1350	A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input, aka 'Git for Visual Studio Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1349, CVE-2019-1352, CVE-2019-1354, CVE-2019-1387.
CVE-2019-13509	In Docker CE and EE before 18.09.8 (as well as Docker EE before 17.06.2-ee-23 and 18.x before 18.03.1-ee-10), Docker Engine in debug mode may sometimes add secrets to the debug log. This applies to a scenario where docker stack deploy is run to redeploy a stack that includes (non external) secrets. It potentially applies to other API users of the stack API if they resend the secret.
CVE-2019-1351	A tampering vulnerability exists when Git for Visual Studio improperly handles virtual drive paths, aka 'Git for Visual Studio Tampering Vulnerability'.
CVE-2019-1352	A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input, aka 'Git for

	Visual Studio Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1349, CVE-2019-1350, CVE-2019-1354, CVE-2019-1387.
CVE-2019-1353	An issue was found in Git before v2.24.1, v2.23.1, v2.22.2, v2.21.1, v2.20.2, v2.19.3, v2.18.2, v2.17.3, v2.16.6, v2.15.4, and v2.14.6. When running Git in the Windows Subsystem for Linux (also known as "WSL") while accessing a working directory on a regular Windows drive, none of the NTFS protections were active.
CVE-2019-1354	A remote code execution vulnerability exists when Git for Visual Studio improperly sanitizes input, aka 'Git for Visual Studio Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2019-1349, CVE-2019-1350, CVE-2019-1352, CVE-2019-1387.
CVE-2019-13616	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in BlitNtоН in video/SDL_blit_N.c when called from SDL_SoftBlit in video/SDL_blit.c.
CVE-2019-13636	In GNU patch through 2.7.6, the following of symlinks is mishandled in certain cases other than input files. This affects inp.c and util.c.
CVE-2019-13638	GNU patch through 2.7.6 is vulnerable to OS shell command injection that can be exploited by opening a crafted patch file that contains an ed style diff payload with shell metacharacters. The ed editor does not need to be present on the vulnerable system. This is different from CVE-2018-1000156.
CVE-2019-13659	IDN spoofing in Omnibox in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2019-13660	UI spoofing in Chromium in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof notifications via a crafted HTML page.
CVE-2019-13661	UI spoofing in Chromium in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof notifications via a crafted HTML page.
CVE-2019-13662	Insufficient policy enforcement in navigations in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2019-13663	IDN spoofing in Omnibox in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2019-13664	Insufficient policy enforcement in Blink in Google Chrome prior to 77.0.3865.75 allowed a remote attacker

	to bypass content security policy via a crafted HTML page.
CVE-2019-13665	Insufficient filtering in Blink in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass multiple file download protection via a crafted HTML page.
CVE-2019-13666	Information leak in storage in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13667	Inappropriate implementation in Omnibox in Google Chrome on iOS prior to 77.0.3865.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-13668	Insufficient policy enforcement in developer tools in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13669	Incorrect data validation in navigation in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-13670	Insufficient data validation in JavaScript in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13671	UI spoofing in Blink in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2019-13673	Insufficient data validation in developer tools in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13674	IDN spoofing in Omnibox in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2019-13675	Insufficient data validation in extensions in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to disable extensions via a crafted HTML page.
CVE-2019-13676	Insufficient policy enforcement in Chromium in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2019-13677	Insufficient policy enforcement in site isolation in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2019-13678	Incorrect data validation in downloads in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.

CVE-2019-13679	Insufficient policy enforcement in PDFium in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to show print dialogs via a crafted PDF file.
CVE-2019-13680	Inappropriate implementation in TLS in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof client IP address to websites via crafted TLS connections.
CVE-2019-13681	Insufficient data validation in downloads in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass download restrictions via a crafted HTML page.
CVE-2019-13682	Insufficient policy enforcement in external protocol handling in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to bypass same origin policy via a crafted HTML page.
CVE-2019-13683	Insufficient policy enforcement in developer tools in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13685	Use after free in sharing view in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13686	Use after free in offline mode in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13687	Use after free in Blink in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13688	Use after free in Blink in Google Chrome prior to 77.0.3865.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13693	Use after free in IndexedDB in Google Chrome prior to 77.0.3865.120 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page.
CVE-2019-13694	Use after free in WebRTC in Google Chrome prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13695	Use after free in audio in Google Chrome on Android prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13696	Use after free in JavaScript in Google Chrome prior to 77.0.3865.120 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13697	Insufficient policy enforcement in performance APIs in Google Chrome prior to 77.0.3865.120 allowed a

	remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13699	Use after free in media in Google Chrome prior to 78.0.3904.70 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13700	Out of bounds memory access in the gamepad API in Google Chrome prior to 78.0.3904.70 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13701	Incorrect implementation in navigation in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-13702	Inappropriate implementation in installer in Google Chrome on Windows prior to 78.0.3904.70 allowed a local attacker to perform privilege escalation via a crafted executable.
CVE-2019-13703	Insufficient policy enforcement in the Omnibox in Google Chrome on Android prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-13704	Insufficient policy enforcement in navigation in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2019-13705	Insufficient policy enforcement in extensions in Google Chrome prior to 78.0.3904.70 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension.
CVE-2019-13706	Out of bounds memory access in PDFium in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-13707	Insufficient validation of untrusted input in intents in Google Chrome on Android prior to 78.0.3904.70 allowed a local attacker to leak files via a crafted application.
CVE-2019-13708	Inappropriate implementation in navigation in Google Chrome on iOS prior to 78.0.3904.70 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-13709	Insufficient policy enforcement in downloads in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to bypass download restrictions via a crafted HTML page.
CVE-2019-13710	Insufficient validation of untrusted input in downloads in Google Chrome prior to 78.0.3904.70 allowed a remote

	attacker to bypass download restrictions via a crafted HTML page.
CVE-2019-13711	Insufficient policy enforcement in JavaScript in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13713	Insufficient policy enforcement in JavaScript in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13714	Insufficient validation of untrusted input in Color Enhancer extension in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to inject CSS into an HTML page via a crafted URL.
CVE-2019-13715	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2019-13716	Insufficient policy enforcement in service workers in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2019-13717	Incorrect security UI in full screen mode in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to hide security UI via a crafted HTML page.
CVE-2019-13718	Insufficient data validation in Omnibox in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2019-13719	Incorrect security UI in full screen mode in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to hide security UI via a crafted HTML page.
CVE-2019-13720	Use after free in WebAudio in Google Chrome prior to 78.0.3904.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13721	Use after free in PDFium in Google Chrome prior to 78.0.3904.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13723	Use after free in WebBluetooth in Google Chrome prior to 78.0.3904.108 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13724	Out of bounds memory access in WebBluetooth in Google Chrome prior to 78.0.3904.108 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13725	Use-after-free in Bluetooth in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to execute arbitrary code via a crafted HTML page.

CVE-2019-13726	Buffer overflow in password manager in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2019-13727	Insufficient policy enforcement in WebSockets in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to bypass same origin policy via a crafted HTML page.
CVE-2019-13728	Out of bounds write in JavaScript in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13729	Use-after-free in WebSockets in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13730	Type confusion in JavaScript in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13732	Use-after-free in WebAudio in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13734	Out of bounds write in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13735	Out of bounds write in JavaScript in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2019-13736	Integer overflow in PDFium in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-13737	Insufficient policy enforcement in autocomplete in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-13738	Insufficient policy enforcement in navigation in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2019-13739	Insufficient policy enforcement in Omnibox in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2019-13740	Incorrect security UI in sharing in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2019-13741	Insufficient validation of untrusted input in Blink in Google Chrome prior to 79.0.3945.79 allowed a local attacker to bypass same origin policy via crafted clipboard content.

CVE-2019-13742	Incorrect security UI in Omnibox in Google Chrome on iOS prior to 79.0.3945.79 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2019-13743	Incorrect security UI in external protocol handling in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2019-13744	Insufficient policy enforcement in cookies in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13745	Insufficient policy enforcement in audio in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-13746	Insufficient policy enforcement in Omnibox in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-13747	Uninitialized data in rendering in Google Chrome on Android prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13748	Insufficient policy enforcement in developer tools in Google Chrome prior to 79.0.3945.79 allowed a local attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-13749	Incorrect security UI in Omnibox in Google Chrome on iOS prior to 79.0.3945.79 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-13750	Insufficient data validation in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to bypass defense-in-depth measures via a crafted HTML page.
CVE-2019-13751	Uninitialized data in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-13752	Out of bounds read in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-13753	Out of bounds read in SQLite in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-13754	Insufficient policy enforcement in extensions in Google Chrome prior to 79.0.3945.79 allowed a remote attacker

	to bypass navigation restrictions via a crafted HTML page.
CVE-2019-13755	Insufficient policy enforcement in extensions in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to disable extensions via a crafted HTML page.
CVE-2019-13756	Incorrect security UI in printing in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2019-13757	Incorrect security UI in Omnibox in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2019-13758	Insufficient policy enforcement in navigation in Google Chrome on Android prior to 79.0.3945.79 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2019-13759	Incorrect security UI in interstitials in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2019-13761	Incorrect security UI in Omnibox in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2019-13762	Insufficient policy enforcement in downloads in Google Chrome on Windows prior to 79.0.3945.79 allowed a local attacker to spoof downloaded files via local code.
CVE-2019-13763	Insufficient policy enforcement in payments in Google Chrome prior to 79.0.3945.79 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page.
CVE-2019-13764	Type confusion in JavaScript in Google Chrome prior to 79.0.3945.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13765	Use-after-free in content delivery manager in Google Chrome prior to 78.0.3904.70 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13766	Use-after-free in accessibility in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-13767	Use after free in media picker in Google Chrome prior to 79.0.3945.88 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-1387	An issue was found in Git before v2.24.1, v2.23.1, v2.22.2, v2.21.1, v2.20.2, v2.19.3, v2.18.2, v2.17.3, v2.16.6, v2.15.4, and v2.14.6. Recursive clones are currently affected by a vulnerability that is caused by

	too-lax validation of submodule names, allowing very targeted attacks via remote code execution in recursive clones.
CVE-2019-14287	In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u \\$((0xffffffff))" command.
CVE-2019-14378	ip_reass in ip_input.c in libslirp 4.0.0 has a heap-based buffer overflow via a large packet because it mishandles a case involving the first fragment.
CVE-2019-14494	An issue was discovered in Poppler through 0.78.0. There is a divide-by-zero error in the function SplashOutputDev::tilingPatternFill at SplashOutputDev.cc.
CVE-2019-14558	Insufficient control flow management in BIOS firmware for 8th, 9th, 10th Generation Intel(R) Core(TM), Intel(R) Celeron(R) Processor 4000 & 5000 Series Processors may allow an authenticated user to potentially enable denial of service via adjacent access.
CVE-2019-14559	Uncontrolled resource consumption in EDK II may allow an unauthenticated user to potentially enable denial of service via network access.
CVE-2019-14563	Integer truncation in EDK II may allow an authenticated user to potentially enable escalation of privilege via local access.
CVE-2019-14575	Logic issue in DxelImageVerificationHandler() for EDK II may allow an authenticated user to potentially enable escalation of privilege via local access.
CVE-2019-14586	Use after free vulnerability in EDK II may allow an authenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via adjacent access.
CVE-2019-14587	Logic issue EDK II may allow an unauthenticated user to potentially enable denial of service via adjacent access.
CVE-2019-14809	net/url in Go before 1.11.13 and 1.12.x before 1.12.8 mishandles malformed hosts in URLs, leading to an authorization bypass in some applications. This is related to a Host field with a suffix appearing in neither Hostname() nor Port(), and is related to a non-numeric port number. For example, an attacker can compose a crafted javascript:// URL that results in a hostname of google.com.
CVE-2019-14811	A flaw was found in, ghostscript versions prior to 9.50, in the .pdf_hook_DSC_Creator procedure where it did not properly secure its privileged calls, enabling scripts

	<p>to bypass `'-dSAFER'` restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands.</p>
CVE-2019-14812	<p>A flaw was found in all ghostscript versions 9.x before 9.50, in the .setuserparams2 procedure where it did not properly secure its privileged calls, enabling scripts to bypass `'-dSAFER'` restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands.</p>
CVE-2019-14813	<p>A flaw was found in ghostscript, versions 9.x before 9.50, in the setsystemparams procedure where it did not properly secure its privileged calls, enabling scripts to bypass `'-dSAFER'` restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands.</p>
CVE-2019-14817	<p>A flaw was found in ghostscript versions prior to 9.50, in the .pdfexec token and other procedures where it did not properly secure its privileged calls, enabling scripts to bypass `'-dSAFER'` restrictions. A specially crafted PostScript file could disable security protection and then have access to the file system, or execute arbitrary commands.</p>
CVE-2019-14821	<p>An out-of-bounds access issue was found in the Linux kernel, all versions through 5.3, in the way Linux kernel's KVM hypervisor implements the Coalesced MMIO write operation. It operates on an MMIO ring buffer 'struct kvm_coalesced_mmio' object, wherein write indices 'ring->first' and 'ring->last' value could be supplied by a host user-space process. An unprivileged host user or process with access to '/dev/kvm' device could use this flaw to crash the host kernel, resulting in a denial of service or potentially escalating privileges on the system.</p>
CVE-2019-14822	<p>A flaw was discovered in ibus in versions before 1.5.22 that allows any unprivileged user to monitor and send method calls to the ibus bus of another user due to a misconfiguration in the DBus server setup. A local attacker may use this flaw to intercept all keystrokes of a victim user who is using the graphical interface, change the input method engine, or modify other input related configurations of the victim user.</p>
CVE-2019-14824	<p>A flaw was found in the 'dereference' plugin of 389-ds-base where it could use the 'search' permission to display attribute values. In some configurations, this could allow an authenticated attacker to view private attributes, such as password hashes.</p>
CVE-2019-14834	<p>A vulnerability was found in dnsmasq before version 2.81, where the memory leak allows remote attackers</p>

	<p>to cause a denial of service (memory consumption) via vectors involving DHCP response creation.</p>
CVE-2019-14835	A buffer overflow flaw was found, in versions from 2.6.34 to 5.2.x, in the way Linux kernel's vhost functionality that translates virtqueue buffers to IOVs, logged the buffer descriptors during migration. A privileged guest user able to pass descriptors with invalid length to the host when migration is underway, could use this flaw to increase their privileges on the host.
CVE-2019-14857	A flaw was found in mod_auth_openidc before version 2.4.0.1. An open redirect issue exists in URLs with trailing slashes similar to CVE-2019-3877 in mod_auth_mellon.
CVE-2019-14866	In all versions of cpio before 2.13 does not properly validate input files when generating TAR archives. When cpio is used to create TAR archives from paths an attacker can write to, the resulting archive may contain files with permissions the attacker did not have or in paths he did not have access to. Extracting those archives from a high-privilege user without carefully reviewing them may lead to the compromise of the system.
CVE-2019-14867	A flaw was found in IPA, all 4.6.x versions before 4.6.7, all 4.7.x versions before 4.7.4 and all 4.8.x versions before 4.8.3, in the way the internal function ber_scanf() was used in some components of the IPA server, which parsed kerberos key data. An unauthenticated attacker who could trigger parsing of the krb principal key could cause the IPA server to crash or in some conditions, cause arbitrary code to be executed on the server hosting the IPA server.
CVE-2019-14869	A flaw was found in all versions of ghostscript 9.x before 9.50, where the `charkeys` procedure, where it did not properly secure its privileged calls, enabling scripts to bypass `dSAFER` restrictions. An attacker could abuse this flaw by creating a specially crafted PostScript file that could escalate privileges within the Ghostscript and access files outside of restricted areas or execute commands.
CVE-2019-14906	A flaw was found with the RHSA-2019:3950 erratum, where it did not fix the CVE-2019-13616 SDL vulnerability. This issue only affects Red Hat SDL packages, SDL versions through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer overflow flaw while copying an existing surface into a new optimized one, due to a lack of validation while loading a BMP image, is possible. An application that uses SDL to parse untrusted input files may be vulnerable to this flaw, which could allow an attacker to make the application crash or execute code.

CVE-2019-14907	All samba versions 4.9.x before 4.9.18, 4.10.x before 4.10.12 and 4.11.x before 4.11.5 have an issue where if it is set with "log level = 3" (or above) then the string obtained from the client, after a failed character conversion, is printed. Such strings can be provided during the NTLMSSP authentication exchange. In the Samba AD DC in particular, this may cause a long-lived process(such as the RPC server) to terminate. (In the file server case, the most likely target, smbd, operates as process-per-client and so a crash there is harmless).
CVE-2019-14973	_TIFFCheckMalloc and _TIFFCheckRealloc in tif_aux.c in LibTIFF through 4.0.10 mishandle Integer Overflow checks because they rely on compiler behavior that is undefined by the applicable C standards. This can, for example, lead to an application crash.
CVE-2019-14980	In ImageMagick 7.x before 7.0.8-42 and 6.x before 6.9.10-42, there is a use after free vulnerability in the UnmapBlob function that allows an attacker to cause a denial of service by sending a crafted file.
CVE-2019-14981	In ImageMagick 7.x before 7.0.8-41 and 6.x before 6.9.10-41, there is a divide-by-zero vulnerability in the MeanShiftImage function. It allows an attacker to cause a denial of service by sending a crafted file.
CVE-2019-15139	The XWD image (X Window System window dumping file) parsing component in ImageMagick 7.0.8-41 Q16 allows attackers to cause a denial-of-service (application crash resulting from an out-of-bounds Read) in ReadXWDImage in coders/xwd.c by crafting a corrupted XWD image file, a different vulnerability than CVE-2019-11472.
CVE-2019-15140	coders/mat.c in ImageMagick 7.0.8-43 Q16 allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact by crafting a Matlab image file that is mishandled in ReadImage in MagickCore/constitute.c.
CVE-2019-15141	WriteTIFFImage in coders/tiff.c in ImageMagick 7.0.8-43 Q16 allows attackers to cause a denial-of-service (application crash resulting from a heap-based buffer over-read) via a crafted TIFF image file, related to TIFFRewriteDirectory, TIFFWriteDirectory, TIFFWriteDirectorySec, and TIFFWriteDirectoryTagColormap in tif_dirwrite.c of LibTIFF. NOTE: this occurs because of an incomplete fix for CVE-2019-11597.
CVE-2019-1547	Normally in OpenSSL EC groups always have a cofactor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present.

	<p>This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).</p>
CVE-2019-1549	<p>OpenSSL 1.1.1 introduced a rewritten random number generator (RNG). This was intended to include protection in the event of a fork() system call in order to ensure that the parent and child processes did not share the same RNG state. However this protection was not being used in the default case. A partial mitigation for this issue is that the output from a high precision timer is mixed into the RNG state so the likelihood of a parent and child process sharing state is significantly reduced. If an application already calls OPENSSL_init_crypto() explicitly using OPENSSL_INIT_ATFORK then this problem does not occur at all. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c).</p>
CVE-2019-1551	<p>There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u (Affected 1.0.2-1.0.2t).</p>
CVE-2019-1559	<p>If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable</p>

	"non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q).
CVE-2019-15605	HTTP request smuggling in Node.js 10, 12, and 13 causes malicious payload delivery when transfer-encoding is malformed
CVE-2019-1563	In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/ PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).
CVE-2019-15690	** 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-2019-15691	TigerVNC version prior to 1.10.1 is vulnerable to stack use-after-return, which occurs due to incorrect usage of stack memory in ZRLEDecoder. If decoding routine would throw an exception, ZRLEDecoder may try to access stack variable, which has been already freed during the process of stack unwinding. Exploitation of this vulnerability could potentially result into remote code execution. This attack appear to be exploitable via network connectivity.
CVE-2019-15692	TigerVNC version prior to 1.10.1 is vulnerable to heap buffer overflow. Vulnerability could be triggered from CopyRectDecoder due to incorrect value checks. Exploitation of this vulnerability could potentially result into remote code execution. This attack appear to be exploitable via network connectivity.
CVE-2019-15693	TigerVNC version prior to 1.10.1 is vulnerable to heap buffer overflow, which occurs in TightDecoder::FilterGradient. Exploitation of this vulnerability could potentially result into remote code execution. This attack appear to be exploitable via network connectivity.

CVE-2019-15694	TigerVNC version prior to 1.10.1 is vulnerable to heap buffer overflow, which could be triggered from DecodeManager::decodeRect. Vulnerability occurs due to the signndness error in processing MemOutStream. Exploitation of this vulnerability could potentially result into remote code execution. This attack appear to be exploitable via network connectivity.
CVE-2019-15695	TigerVNC version prior to 1.10.1 is vulnerable to stack buffer overflow, which could be triggered from CMsgReader::readSetCursor. This vulnerability occurs due to insufficient sanitization of PixelFormat. Since remote attacker can choose offset from start of the buffer to start writing his values, exploitation of this vulnerability could potentially result into remote code execution. This attack appear to be exploitable via network connectivity.
CVE-2019-15890	libslirp 4.0.0, as used in QEMU 4.1.0, has a use-after-free in ip_reass in ip_input.c.
CVE-2019-15903	In libexpat before 2.2.8, crafted XML input could fool the parser into changing from DTD parsing to document parsing too early; a consecutive call to XML_GetCurrentLineNumber (or XML_GetCurrentColumnNumber) then resulted in a heap-based buffer over-read.
CVE-2019-15918	An issue was discovered in the Linux kernel before 5.0.10. SMB2_negotiate in fs/cifs/smb2pdu.c has an out-of-bounds read because data structures are incompletely updated after a change from smb30 to smb21.
CVE-2019-16056	An issue was discovered in Python through 2.7.16, 3.x through 3.5.7, 3.6.x through 3.6.9, and 3.7.x through 3.7.4. The email module wrongly parses email addresses that contain multiple @ characters. An application that uses the email module and implements some kind of checks on the From/To headers of a message could be tricked into accepting an email address that should be denied. An attack may be the same as in CVE-2019-11340; however, this CVE applies to Python more generally.
CVE-2019-16163	Oniguruma before 6.9.3 allows Stack Exhaustion in regcomp.c because of recursion in reparse.c.
CVE-2019-16168	In SQLite through 3.29.0, whereLoopAddBtreeIndex in sqlite3.c can crash a browser or other application because of missing validation of a sqlite_stat1 sz field, aka a "severe division by zero in the query planner."
CVE-2019-16276	Go before 1.12.10 and 1.13.x before 1.13.1 allow HTTP Request Smuggling.
CVE-2019-16707	Hunspell 1.7.0 has an invalid read operation in SuggestMgr::leftcommonsubstring in suggestmgr.cxx.

CVE-2019-16708	ImageMagick 7.0.8-35 has a memory leak in magick/xwindow.c, related to XCreateImage.
CVE-2019-16709	ImageMagick 7.0.8-35 has a memory leak in coders/dps.c, as demonstrated by XCreateImage.
CVE-2019-16710	ImageMagick 7.0.8-35 has a memory leak in coders/dot.c, as demonstrated by AcquireMagickMemory in MagickCore/memory.c.
CVE-2019-16711	ImageMagick 7.0.8-40 has a memory leak in Huffman2DEncodeImage in coders/ps2.c.
CVE-2019-16712	ImageMagick 7.0.8-43 has a memory leak in Huffman2DEncodeImage in coders/ps3.c, as demonstrated by WritePS3Image.
CVE-2019-16713	ImageMagick 7.0.8-43 has a memory leak in coders/dot.c, as demonstrated by PingImage in MagickCore/constitute.c.
CVE-2019-16865	An issue was discovered in Pillow before 6.2.0. When reading specially crafted invalid image files, the library can either allocate very large amounts of memory or take an extremely long period of time to process the image.
CVE-2019-16884	runc through 1.0.0-rc8, as used in Docker through 19.03.2-ce and other products, allows AppArmor restriction bypass because libcontainer/rootfs_linux.go incorrectly checks mount targets, and thus a malicious Docker image can mount over a /proc directory.
CVE-2019-17005	The plain text serializer used a fixed-size array for the number of elements it could process; however it was possible to overflow the static-sized array leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.3, Firefox ESR < 68.3, and Firefox < 71.
CVE-2019-17006	In Network Security Services (NSS) before 3.46, several cryptographic primitives had missing length checks. In cases where the application calling the library did not perform a sanity check on the inputs it could result in a crash due to a buffer overflow.
CVE-2019-17008	When using nested workers, a use-after-free could occur during worker destruction. This resulted in a potentially exploitable crash. This vulnerability affects Thunderbird < 68.3, Firefox ESR < 68.3, and Firefox < 71.
CVE-2019-17010	Under certain conditions, when checking the Resist Fingerprinting preference during device orientation checks, a race condition could have caused a use-after-free and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.3, Firefox ESR < 68.3, and Firefox < 71.
CVE-2019-17011	Under certain conditions, when retrieving a document from a DocShell in the antitracking code, a race

	condition could cause a use-after-free condition and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.3, Firefox ESR < 68.3, and Firefox < 71.
CVE-2019-17012	Mozilla developers reported memory safety bugs present in Firefox 70 and Firefox ESR 68.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.3, Firefox ESR < 68.3, and Firefox < 71.
CVE-2019-17016	When pasting a <style> tag from the clipboard into a rich text editor, the CSS sanitizer incorrectly rewrites a @namespace rule. This could allow for injection into certain types of websites resulting in data exfiltration. This vulnerability affects Firefox ESR < 68.4 and Firefox < 72.
CVE-2019-17017	Due to a missing case handling object types, a type confusion vulnerability could occur, resulting in a crash. We presume that with enough effort that it could be exploited to run arbitrary code. This vulnerability affects Firefox ESR < 68.4 and Firefox < 72.
CVE-2019-17022	When pasting a <style> tag from the clipboard into a rich text editor, the CSS sanitizer does not escape < and > characters. Because the resulting string is pasted directly into the text node of the element this does not result in a direct injection into the webpage; however, if a webpage subsequently copies the node's innerHTML, assigning it to another innerHTML, this would result in an XSS vulnerability. Two WYSIWYG editors were identified with this behavior, more may exist. This vulnerability affects Firefox ESR < 68.4 and Firefox < 72.
CVE-2019-17023	After a HelloRetryRequest has been sent, the client may negotiate a lower protocol than TLS 1.3, resulting in an invalid state transition in the TLS State Machine. If the client gets into this state, incoming Application Data records will be ignored. This vulnerability affects Firefox < 72.
CVE-2019-17024	Mozilla developers reported memory safety bugs present in Firefox 71 and Firefox ESR 68.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 68.4 and Firefox < 72.
CVE-2019-17026	Incorrect alias information in IonMonkey JIT compiler for setting array elements could lead to a type confusion. We are aware of targeted attacks in the wild

	abusing this flaw. This vulnerability affects Firefox ESR < 68.4.1, Thunderbird < 68.4.1, and Firefox < 72.0.1.
CVE-2019-17041	An issue was discovered in Rsyslog v8.1908.0. contrib/pmaixforwardedfrom/pmaixforwardedfrom.c has a heap overflow in the parser for AIX log messages. The parser tries to locate a log message delimiter (in this case, a space or a colon) but fails to account for strings that do not satisfy this constraint. If the string does not match, then the variable lenMsg will reach the value zero and will skip the sanity check that detects invalid log messages. The message will then be considered valid, and the parser will eat up the nonexistent colon delimiter. In doing so, it will decrement lenMsg, a signed integer, whose value was zero and now becomes minus one. The following step in the parser is to shift left the contents of the message. To do this, it will call memmove with the right pointers to the target and destination strings, but the lenMsg will now be interpreted as a huge value, causing a heap overflow.
CVE-2019-17042	An issue was discovered in Rsyslog v8.1908.0. contrib/pmcisconames/pmcisconames.c has a heap overflow in the parser for Cisco log messages. The parser tries to locate a log message delimiter (in this case, a space or a colon), but fails to account for strings that do not satisfy this constraint. If the string does not match, then the variable lenMsg will reach the value zero and will skip the sanity check that detects invalid log messages. The message will then be considered valid, and the parser will eat up the nonexistent colon delimiter. In doing so, it will decrement lenMsg, a signed integer, whose value was zero and now becomes minus one. The following step in the parser is to shift left the contents of the message. To do this, it will call memmove with the right pointers to the target and destination strings, but the lenMsg will now be interpreted as a huge value, causing a heap overflow.
CVE-2019-17185	In FreeRADIUS 3.0.x before 3.0.20, the EAP-pwd module used a global OpenSSL BN_CTX instance to handle all handshakes. This mean multiple threads use the same BN_CTX instance concurrently, resulting in crashes when concurrent EAP-pwd handshakes are initiated. This can be abused by an adversary as a Denial-of-Service (DoS) attack.
CVE-2019-17402	Exiv2 0.27.2 allows attackers to trigger a crash in Exiv2::getULong in types.cpp when called from Exiv2::Internal::CifffDirectory::readDirectory in crwimage_int.cpp, because there is no validation of the relationship of the total size to the offset and size.
CVE-2019-17498	In libssh2 v1.9.0 and earlier versions, the SSH_MSG_DISCONNECT logic in packet.c has an integer overflow in a bounds check, enabling an

	attacker to specify an arbitrary (out-of-bounds) offset for a subsequent memory read. A crafted SSH server may be able to disclose sensitive information or cause a denial of service condition on the client system when a user connects to the server.
CVE-2019-17540	ImageMagick before 7.0.8-54 has a heap-based buffer overflow in ReadPSInfo in coders/ps.c.
CVE-2019-17541	ImageMagick before 7.0.8-55 has a use-after-free in DestroyStringInfo in MagickCore/string.c because the error manager is mishandled in coders/jpeg.c.
CVE-2019-17546	tif_getimage.c in LibTIFF through 4.0.10, as used in GDAL through 3.0.1 and other products, has an integer overflow that potentially causes a heap-based buffer overflow via a crafted RGBA image, related to a "Negative-size-param" condition.
CVE-2019-17558	Apache Solr 5.0.0 to Apache Solr 8.3.1 are vulnerable to a Remote Code Execution through the VelocityResponseWriter. A Velocity template can be provided through Velocity templates in a configset `velocity/` directory or as a parameter. A user defined configset could contain renderable, potentially malicious, templates. Parameter provided templates are disabled by default, but can be enabled by setting `params.resource.loader.enabled` by defining a response writer with that setting set to `true`. Defining a response writer requires configuration API access. Solr 8.4 removed the params resource loader entirely, and only enables the configset-provided template rendering when the configset is `trusted` (has been uploaded by an authenticated user).
CVE-2019-17567	Apache HTTP Server versions 2.4.6 to 2.4.46 mod_proxy_wstunnel configured on an URL that is not necessarily Upgraded by the origin server was tunneling the whole connection regardless, thus allowing for subsequent requests on the same connection to pass through with no HTTP validation, authentication or authorization possibly configured.
CVE-2019-17626	ReportLab through 3.5.26 allows remote code execution because of toColor(eval(arg)) in colors.py, as demonstrated by a crafted XML document with '<span color="" followed by arbitrary Python code.
CVE-2019-17638	In Eclipse Jetty, versions 9.4.27.v20200227 to 9.4.29.v20200521, in case of too large response headers, Jetty throws an exception to produce an HTTP 431 error. When this happens, the ByteBuffer containing the HTTP response headers is released back to the ByteBufferPool twice. Because of this double release, two threads can acquire the same ByteBuffer from the pool and while thread1 is about to use the ByteBuffer to write response1 data, thread2 fills the ByteBuffer with other data. Thread1 then

	<p>proceeds to write the buffer that now contains different data. This results in client1, which issued request1 seeing data from another request or response which could contain sensitive data belonging to client2 (HTTP session ids, authentication credentials, etc.). If the Jetty version cannot be upgraded, the vulnerability can be significantly reduced by configuring a responseHeaderSize significantly larger than the requestHeaderSize (12KB responseHeaderSize and 8KB requestHeaderSize).</p>
CVE-2019-18197	In xsItCopyText in transform.c in libxslt 1.1.33, a pointer variable isn't reset under certain circumstances. If the relevant memory area happened to be freed and reused in a certain way, a bounds check could fail and memory outside a buffer could be written to, or uninitialized data could be disclosed.
CVE-2019-18218	cdf_read_property_info in cdf.c in file through 5.37 does not restrict the number of CDF_VECTOR elements, which allows a heap-based buffer overflow (4-byte out-of-bounds write).
CVE-2019-18224	idn2_to_ascii_4i in lib/lookup.c in GNU libidn2 before 2.1.1 has a heap-based buffer overflow via a long domain string.
CVE-2019-18397	A buffer overflow in the fribri _get_par_embedding_levels_ex() function in lib/fribidi-bidi.c of GNU FriBidi through 1.0.7 allows an attacker to cause a denial of service or possibly execute arbitrary code by delivering crafted text content to a user, when this content is then rendered by an application that uses FriBidi for text layout calculations. Examples include any GNOME or GTK+ based application that uses Pango for text layout, as this internally uses FriBidi for bidirectional text layout. For example, the attacker can construct a crafted text file to be opened in GEdit, or a crafted IRC message to be viewed in HexChat.
CVE-2019-18408	archive_read_format_rar_read_data in archive_read_support_format_rar.c in libarchive before 3.4.0 has a use-after-free in a certain ARCHIVE_FAILED situation, related to Ppmf7_DecodeSymbol.
CVE-2019-18634	In Sudo before 1.8.26, if pwfeedback is enabled in /etc/sudoers, users can trigger a stack-based buffer overflow in the privileged sudo process. (pwfeedback is a default setting in Linux Mint and elementary OS; however, it is NOT the default for upstream and many other packages, and would exist only if enabled by an administrator.) The attacker needs to deliver a long string to the stdin of getln() in tgetpass.c.
CVE-2019-18679	An issue was discovered in Squid 2.x, 3.x, and 4.x through 4.8. Due to incorrect data management, it is

	vulnerable to information disclosure when processing HTTP Digest Authentication. Nonce tokens contain the raw byte value of a pointer that sits within heap memory allocation. This information reduces ASLR protections and may aid attackers isolating memory areas to target for remote code execution attacks.
CVE-2019-18808	A memory leak in the ccp_run_sha_cmd() function in drivers/crypto/ccp/ccp-ops.c in the Linux kernel through 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-128c66429247.
CVE-2019-19012	An integer overflow in the search_in_range function in regexec.c in Oniguruma 6.x before 6.9.4_rc2 leads to an out-of-bounds read, in which the offset of this read is under the control of an attacker. (This only affects the 32-bit compiled version). Remote attackers can cause a denial-of-service or information disclosure, or possibly have unspecified other impact, via a crafted regular expression.
CVE-2019-19054	A memory leak in the cx23888_ir_probe() function in drivers/media/pci/cx23885/cx23888-ir.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering kfifo_alloc() failures, aka CID-a7b2df76b42b.
CVE-2019-19060	A memory leak in the adis_update_scan_mode() function in drivers/iio imu/adis_buffer.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-ab612b1daf41.
CVE-2019-19061	A memory leak in the adis_update_scan_mode_burst() function in drivers/iio imu/adis_buffer.c in the Linux kernel before 5.3.9 allows attackers to cause a denial of service (memory consumption), aka CID-9c0530e898f3.
CVE-2019-19062	A memory leak in the crypto_report() function in crypto/crypto_user_base.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption) by triggering crypto_report_alg() failures, aka CID-ffdde5932042.
CVE-2019-19073	Memory leaks in drivers/net/wireless/ath/ath9k/htc_hst.c in the Linux kernel through 5.3.11 allow attackers to cause a denial of service (memory consumption) by triggering wait_for_completion_timeout() failures. This affects the htc_config_pipe_credits() function, the htc_setup_complete() function, and the htc_connect_service() function, aka CID-853acf7caf10.
CVE-2019-19074	A memory leak in the ath9k_wmi_cmd() function in drivers/net/wireless/ath/ath9k/wmi.c in the Linux kernel through 5.3.11 allows attackers to cause a denial of service (memory consumption), aka CID-728c1e2a05e4.

CVE-2019-19204	An issue was discovered in Oniguruma 6.x before 6.9.4_rc2. In the function <code>fetch_interval_quantifier</code> (formerly known as <code>fetch_range_quantifier</code>) in <code>regparse.c</code> , PFETCH is called without checking PEND. This leads to a heap-based buffer over-read.
CVE-2019-19246	Oniguruma through 6.9.3, as used in PHP 7.3.x and other products, has a heap-based buffer over-read in <code>str_lower_case_match</code> in <code>regexec.c</code> .
CVE-2019-19319	In the Linux kernel before 5.2, a setxattr operation, after a mount of a crafted ext4 image, can cause a slab-out-of-bounds write access because of an <code>ext4_xattr_set_entry</code> use-after-free in <code>fs/ext4/xattr.c</code> when a large <code>old_size</code> value is used in a <code>memset</code> call, aka CID-345c0dbf3a30.
CVE-2019-19332	An out-of-bounds memory write issue was found in the Linux Kernel, version 3.13 through 5.4, in the way the Linux kernel's KVM hypervisor handled the ' <code>KVM_GET_EMULATED_CPUID</code> ' ioctl(2) request to get CPUID features emulated by the KVM hypervisor. A user or process able to access the '/dev/kvm' device could use this flaw to crash the system, resulting in a denial of service.
CVE-2019-19448	In the Linux kernel 5.0.21 and 5.3.11, mounting a crafted btrfs filesystem image, performing some operations, and then making a syncfs system call can lead to a use-after-free in <code>try_merge_free_space</code> in <code>fs/btrfs/free-space-cache.c</code> because the pointer to a left data structure can be the same as the pointer to a right data structure.
CVE-2019-19462	<code>relay_open</code> in <code>kernel/relay.c</code> in the Linux kernel through 5.4.1 allows local users to cause a denial of service (such as relay blockage) by triggering a NULL <code>alloc_percpu</code> result.
CVE-2019-19604	Arbitrary command execution is possible in Git before 2.20.2, 2.21.x before 2.21.1, 2.22.x before 2.22.2, 2.23.x before 2.23.1, and 2.24.x before 2.24.1 because a "git submodule update" operation can run commands found in the .gitmodules file of a malicious repository.
CVE-2019-19746	<code>make_arrow</code> in <code>arrow.c</code> in Xfig fig2dev 3.2.7b allows a segmentation fault and out-of-bounds write because of an integer overflow via a large arrow type.
CVE-2019-19768	In the Linux kernel 5.4.0-rc2, there is a use-after-free (read) in the <code>__blk_add_trace</code> function in <code>kernel/trace/blktrace.c</code> (which is used to fill out a <code>blk_io_trace</code> structure and place it in a per-cpu sub-buffer).
CVE-2019-19770	** DISPUTED ** In the Linux kernel 4.19.83, there is a use-after-free (read) in the <code>debugfs_remove</code> function in <code>fs/debugfs/inode.c</code> (which is used to remove a file or directory in debugfs that was previously created with a call to another debugfs function such as

	debugfs_create_file). NOTE: Linux kernel developers dispute this issue as not being an issue with debugfs, instead this is an issue with misuse of debugfs within blktrace.
CVE-2019-19797	read_colordef in read.c in Xfig fig2dev 3.2.7b has an out-of-bounds write.
CVE-2019-19813	In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image, performing some operations, and then making a syncfs system call can lead to a use-after-free in __mutex_lock in kernel/locking/mutex.c. This is related to mutex_can_spin_on_owner in kernel/locking/mutex.c, __btrfs_qgroup_free_meta in fs/btrfs/qgroup.c, and btrfs_insert_delayed_items in fs/btrfs/delayed-inode.c.
CVE-2019-19816	In the Linux kernel 5.0.21, mounting a crafted btrfs filesystem image and performing some operations can cause slab-out-of-bounds write access in __btrfs_map_block in fs/btrfs/volumes.c, because a value of 1 for the number of data stripes is mishandled.
CVE-2019-19880	exprListAppendList in window.c in SQLite 3.30.1 allows attackers to trigger an invalid pointer dereference because constant integer values in ORDER BY clauses of window definitions are mishandled.
CVE-2019-19921	runc through 1.0.0-rc9 has Incorrect Access Control leading to Escalation of Privileges, related to libcontainer/rootfs_linux.go. To exploit this, an attacker must be able to spawn two containers with custom volume-mount configurations, and be able to run custom images. (This vulnerability does not affect Docker due to an implementation detail that happens to block the attack.)
CVE-2019-19923	flattenSubquery in select.c in SQLite 3.30.1 mishandles certain uses of SELECT DISTINCT involving a LEFT JOIN in which the right-hand side is a view. This can cause a NULL pointer dereference (or incorrect results).
CVE-2019-19925	zipfileUpdate in ext/misc/zipfile.c in SQLite 3.30.1 mishandles a NULL pathname during an update of a ZIP archive.
CVE-2019-19926	multiSelect in select.c in SQLite 3.30.1 mishandles certain errors during parsing, as demonstrated by errors from sqlite3WindowRewrite() calls. NOTE: this vulnerability exists because of an incomplete fix for CVE-2019-19880.
CVE-2019-19948	In ImageMagick 7.0.8-43 Q16, there is a heap-based buffer overflow in the function WriteSGIImage of coders/sgi.c.
CVE-2019-19949	In ImageMagick 7.0.8-43 Q16, there is a heap-based buffer over-read in the function WritePNGImage of

	coders/png.c, related to Magick_png_write_raw_profile and LocaleNCompare.
CVE-2019-19956	xmlParseBalancedChunkMemoryRecover in parser.c in libxml2 before 2.9.10 has a memory leak related to newDoc->oldNs.
CVE-2019-20044	In Zsh before 5.8, attackers able to execute commands can regain privileges dropped by the --no-PRIVILEGED option. Zsh fails to overwrite the saved uid, so the original privileges can be restored by executing MODULE_PATH=/dir/with/module zmodload with a module that calls setuid().
CVE-2019-20096	In the Linux kernel before 5.1, there is a memory leak in __feat_register_sp() in net/dccp/feat.c, which may cause denial of service, aka CID-1d3ff0950e2b.
CVE-2019-20382	QEMU 4.1.0 has a memory leak in zrle_compress_data in ui/vnc-enc-zrle.c during a VNC disconnect operation because libz is misused, resulting in a situation where memory allocated in deflateInit2 is not freed in deflateEnd.
CVE-2019-20386	An issue was discovered in button_open in login/loginbutton.c in systemd before 243. When executing the udevadm trigger command, a memory leak may occur.
CVE-2019-20388	xmlSchemaPreRun in xmlschemas.c in libxml2 2.9.10 allows an xmlSchemaValidateStream memory leak.
CVE-2019-20479	A flaw was found in mod_auth_openidc before version 2.4.1. An open redirect issue exists in URLs with a slash and backslash at the beginning.
CVE-2019-20485	qemu/qemu_driver.c in libvirt before 6.0.0 mishandles the holding of a monitor job during a query to a guest agent, which allows attackers to cause a denial of service (API blockage).
CVE-2019-20503	usrstcp before 2019-12-20 has out-of-bounds reads in sctp_load_addresses_from_init.
CVE-2019-20907	In Lib/tarfile.py in Python through 3.8.3, an attacker is able to craft a TAR archive leading to an infinite loop when opened by tarfile.open, because _proc_pax lacks header validation.
CVE-2019-20916	The pip package before 19.2 for Python allows Directory Traversal when a URL is given in an install command, because a Content-Disposition header can have .. / in a filename, as demonstrated by overwriting the /root/.ssh/authorized_keys file. This occurs in _download_http_url in _internal/download.py.
CVE-2019-2422	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u201, 8u192 and 11.0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise

	<p>Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).</p>
CVE-2019-2426	<p>Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 7u201, 8u192 and 11.0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).</p>
CVE-2019-2449	<p>Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). The supported version that is affected is Java SE: 8u192. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability</p>

	impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L).
CVE-2019-25013	The iconv feature in the GNU C Library (aka glibc or libc6) through 2.32, when processing invalid multi-byte input sequences in the EUC-KR encoding, may have a buffer over-read.
CVE-2019-2503	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection Handling). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Difficult to exploit vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:H).
CVE-2019-25032	** DISPUTED ** Unbound before 1.9.5 allows an integer overflow in the regional allocator via regional_alloc. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited.
CVE-2019-25034	** DISPUTED ** Unbound before 1.9.5 allows an integer overflow in sldns_str2wire_dname_buf_origin, leading to an out-of-bounds write. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited.
CVE-2019-25035	** DISPUTED ** Unbound before 1.9.5 allows an out-of-bounds write in sldns_bget_token_par. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited.
CVE-2019-25036	** DISPUTED ** Unbound before 1.9.5 allows an assertion failure and denial of service in synth_cname. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited.
CVE-2019-25037	** DISPUTED ** Unbound before 1.9.5 allows an assertion failure and denial of service in dname_pkt_copy via an invalid packet. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited.

CVE-2019-25038	** DISPUTED ** Unbound before 1.9.5 allows an integer overflow in a size calculation in dnsrypt/dnsrypt.c. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited.
CVE-2019-25039	** DISPUTED ** Unbound before 1.9.5 allows an integer overflow in a size calculation in respip/respip.c. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited.
CVE-2019-25040	** DISPUTED ** Unbound before 1.9.5 allows an infinite loop via a compressed name in dname_pkt_copy. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited.
CVE-2019-25041	** DISPUTED ** Unbound before 1.9.5 allows an assertion failure via a compressed name in dname_pkt_copy. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited.
CVE-2019-25042	** DISPUTED ** Unbound before 1.9.5 allows an out-of-bounds write via a compressed name in rdata_copy. NOTE: The vendor disputes that this is a vulnerability. Although the code may be vulnerable, a running Unbound installation cannot be remotely or locally exploited.
CVE-2019-2529	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 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-2019-2602	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or

	frequently repeatable crash (complete DOS) of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2019-2614	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 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-2019-2627	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 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-2019-2684	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 7u211, 8u202, 11.0.2 and 12; Java SE Embedded: 8u201. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity)

	impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).
CVE-2019-2697	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 7u211 and 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2019-2698	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 7u211 and 8u202. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2019-2737	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Pluggable Auth). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 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-2019-2739	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges).

	Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 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 as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2019-2740	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: XML). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 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-2019-2745	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 7u221, 8u212 and 11.0.3. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE executes to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2019-2762	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Utilities). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of

	<p>service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).</p>
CVE-2019-2766	<p>Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).</p>
CVE-2019-2769	<p>Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Utilities). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS</p>

	3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2786	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:H).
CVE-2019-2805	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.6.44 and prior, 5.7.26 and prior and 8.0.16 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-2019-2816	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 7u221, 8u212, 11.0.3 and 12.0.1; Java SE Embedded: 8u211. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications

	or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2019-2818	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 11.0.3 and 12.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).
CVE-2019-2821	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JSSE). Supported versions that are affected are Java SE: 11.0.3 and 12.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:N/A:N).
CVE-2019-2842	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: JCE). The supported version that is affected is Java SE: 8u212. Difficult to exploit vulnerability allows unauthenticated attacker with

	<p>network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).</p>
CVE-2019-2853	<p>Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.4. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Outside In Technology. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data as well as unauthorized read access to a subset of Oracle Outside In Technology accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Outside In Technology. Note: Outside In Technology is a suite of software development kits (SDKs). The protocol and CVSS score depend on the software that uses the Outside In Technology code. The CVSS score assumes that the software passes data received over a network directly to Outside In Technology code, but if data is not received over a network the CVSS score may be lower. CVSS 3.0 Base Score 7.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L).</p>
CVE-2019-2894	<p>Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: 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.</p>

	This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2019-2945	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. 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 ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L).
CVE-2019-2949	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Kerberos). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).

CVE-2019-2958	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).
CVE-2019-2962	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2964	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Concurrency). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by

	supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2973	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2974	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 5.6.45 and prior, 5.7.27 and prior and 8.0.17 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-2019-2975	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions that are affected are Java SE: 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications

	or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:L).
CVE-2019-2977	Vulnerability in the Java SE product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 11.0.4 and 13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.8 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:L).
CVE-2019-2978	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2981	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded:

	8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2983	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2987	Vulnerability in the Java SE product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 11.0.4 and 13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7

	(Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2988	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability 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 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2019-2989	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS v3.0 Base Score 6.8 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:H/A:N).
CVE-2019-2992	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13; Java SE Embedded: 8u221. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks

	<p>of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability 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 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).</p>
CVE-2019-2999	<p>Vulnerability in the Java SE product of Oracle Java SE (component: Javadoc). Supported versions that are affected are Java SE: 7u231, 8u221, 11.0.4 and 13. 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 unauthorized update, insert or delete access to some of Java SE accessible data as well as unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.7 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N).</p>
CVE-2019-3016	<p>In a Linux KVM guest that has PV TLB enabled, a process in the guest kernel may be able to read memory locations from another process in the same guest. This problem is limit to the host running linux kernel 4.10 with a guest running linux kernel 4.16 or later. The problem mainly affects AMD processors but Intel CPUs cannot be ruled out.</p>
CVE-2019-3459	<p>A heap address information leak while using L2CAP_GET_CONF_OPT was discovered in the Linux kernel before 5.1-rc1.</p>
CVE-2019-3460	<p>A heap data info leak in multiple locations including L2CAP_PARSE_CONF_RSP was found in the Linux kernel before 5.1-rc1.</p>

CVE-2019-3695	A Improper Control of Generation of Code vulnerability in the packaging of pcp of SUSE Linux Enterprise High Performance Computing 15-ESPOS, SUSE Linux Enterprise High Performance Computing 15-LTSS, SUSE Linux Enterprise Module for Development Tools 15, SUSE Linux Enterprise Module for Development Tools 15-SP1, SUSE Linux Enterprise Module for Open Buildservice Development Tools 15, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 15, SUSE Linux Enterprise Software Development Kit 12-SP4, SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap 15.1 allows the user pcp to run code as root by placing it into /var/log/pcp/configs.sh This issue affects: SUSE Linux Enterprise High Performance Computing 15-ESPOS pcp versions prior to 3.11.9-5.8.1. SUSE Linux Enterprise High Performance Computing 15-LTSS pcp versions prior to 3.11.9-5.8.1. SUSE Linux Enterprise Module for Development Tools 15 pcp versions prior to 3.11.9-5.8.1. SUSE Linux Enterprise Module for Development Tools 15-SP1 pcp versions prior to 4.3.1-3.5.3. SUSE Linux Enterprise Module for Open Buildservice Development Tools 15 pcp versions prior to 3.11.9-5.8.1. SUSE Linux Enterprise Server 15-LTSS pcp versions prior to 3.11.9-5.8.1. SUSE Linux Enterprise Server for SAP 15 pcp versions prior to 3.11.9-5.8.1. SUSE Linux Enterprise Software Development Kit 12-SP4 pcp versions prior to 3.11.9-6.14.1. SUSE Linux Enterprise Software Development Kit 12-SP5 pcp versions prior to 3.11.9-6.14.1. openSUSE Leap 15.1 pcp versions prior to 4.3.1-1p151.2.3.1.
CVE-2019-3696	A Improper Limitation of a Pathname to a Restricted Directory vulnerability in the packaging of pcp of SUSE Linux Enterprise High Performance Computing 15-ESPOS, SUSE Linux Enterprise High Performance Computing 15-LTSS, SUSE Linux Enterprise Module for Development Tools 15, SUSE Linux Enterprise Module for Development Tools 15-SP1, SUSE Linux Enterprise Module for Open Buildservice Development Tools 15, SUSE Linux Enterprise Server 15-LTSS, SUSE Linux Enterprise Server for SAP 15, SUSE Linux Enterprise Software Development Kit 12-SP4, SUSE Linux Enterprise Software Development Kit 12-SP5; openSUSE Leap 15.1 allows local user pcp to overwrite arbitrary files with arbitrary content. This issue affects: SUSE Linux Enterprise High Performance Computing 15-ESPOS pcp versions prior to 3.11.9-5.8.1. SUSE Linux Enterprise High Performance Computing 15-LTSS pcp versions prior to 3.11.9-5.8.1. SUSE Linux Enterprise Module for Development Tools 15 pcp versions prior to 3.11.9-5.8.1. SUSE Linux Enterprise Module for Development Tools 15-SP1 pcp

	versions prior to 4.3.1-3.5.3. SUSE Linux Enterprise Module for Open Buildservice Development Tools 15 pcp versions prior to 3.11.9-5.8.1. SUSE Linux Enterprise Server 15-LTSS pcp versions prior to 3.11.9-5.8.1. SUSE Linux Enterprise Server for SAP 15 pcp versions prior to 3.11.9-5.8.1. SUSE Linux Enterprise Software Development Kit 12-SP4 pcp versions prior to 3.11.9-6.14.1. SUSE Linux Enterprise Software Development Kit 12-SP5 pcp versions prior to 3.11.9-6.14.1. openSUSE Leap 15.1 pcp versions prior to 4.3.1-lp151.2.3.1.
CVE-2019-3811	A vulnerability was found in sssd. If a user was configured with no home directory set, sssd would return '/' (the root directory) instead of "" (the empty string / no home directory). This could impact services that restrict the user's filesystem access to within their home directory through chroot() etc. All versions before 2.1 are vulnerable.
CVE-2019-3813	Spice, versions 0.5.2 through 0.14.1, are vulnerable to an out-of-bounds read due to an off-by-one error in memslot_get_virt. This may lead to a denial of service, or, in the worst case, code-execution by unauthenticated attackers.
CVE-2019-3814	It was discovered that Dovecot before versions 2.2.36.1 and 2.3.4.1 incorrectly handled client certificates. A remote attacker in possession of a valid certificate with an empty username field could possibly use this issue to impersonate other users.
CVE-2019-3815	A memory leak was discovered in the backport of fixes for CVE-2018-16864 in Red Hat Enterprise Linux. Function dispatch_message_real() in journald-server.c does not free the memory allocated by set_iovec_field_free() to store the '_CMDLINE=' entry. A local attacker may use this flaw to make systemd-journald crash. This issue only affects versions shipped with Red Hat Enterprise since v219-62.2.
CVE-2019-3816	Openwsman, versions up to and including 2.6.9, are vulnerable to arbitrary file disclosure because the working directory of openwsmand daemon was set to root directory. A remote, unauthenticated attacker can exploit this vulnerability by sending a specially crafted HTTP request to openwsman server.
CVE-2019-3820	It was discovered that the gnome-shell lock screen since version 3.15.91 did not properly restrict all contextual actions. An attacker with physical access to a locked workstation could invoke certain keyboard shortcuts, and potentially other actions.
CVE-2019-3822	curl versions from 7.36.0 to before 7.64.0 are vulnerable to a stack-based buffer overflow. The function creating an outgoing NTLM type-3 header ('lib/vauth/

	ntlm.c:Curl_auth_create_ntlm_type3_message(`), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening. This output data can grow larger than the local buffer if very large 'nt response' data is extracted from a previous NTLMv2 header provided by the malicious or broken HTTP server. Such a 'large value' needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header.
CVE-2019-3823	libcurl versions from 7.34.0 to before 7.64.0 are vulnerable to a heap out-of-bounds read in the code handling the end-of-response for SMTP. If the buffer passed to `smtp_endofresp()` isn't NUL terminated and contains no character ending the parsed number, and 'len' is set to 5, then the `strtol()` call reads beyond the allocated buffer. The read contents will not be returned to the caller.
CVE-2019-3833	Openwsman, versions up to and including 2.6.9, are vulnerable to infinite loop in process_connection() when parsing specially crafted HTTP requests. A remote, unauthenticated attacker can exploit this vulnerability by sending malicious HTTP request to cause denial of service to openwsman server.
CVE-2019-3835	It was found that the superexec operator was available in the internal dictionary in ghostscript before 9.27. A specially crafted PostScript file could use this flaw in order to, for example, have access to the file system outside of the constraints imposed by -dSAFER.
CVE-2019-3838	It was found that the forceput operator could be extracted from the DefineResource method in ghostscript before 9.27. A specially crafted PostScript file could use this flaw in order to, for example, have access to the file system outside of the constraints imposed by -dSAFER.
CVE-2019-3839	It was found that in ghostscript some privileged operators remained accessible from various places after the CVE-2019-6116 fix. A specially crafted PostScript file could use this flaw in order to, for example, have access to the file system outside of the constraints imposed by -dSAFER. Ghostscript versions before 9.27 are vulnerable.
CVE-2019-3840	A NULL pointer dereference flaw was discovered in libvirt before version 5.0.0 in the way it gets interface information through the QEMU agent. An attacker in a guest VM can use this flaw to crash libvirtd and cause a denial of service.

CVE-2019-3855	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2019-3856	An integer overflow flaw, which could lead to an out of bounds write, was discovered in libssh2 before 1.8.1 in the way keyboard prompt requests are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2019-3857	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit signal are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2019-3858	An out of bounds read flaw was discovered in libssh2 before 1.8.1 when a specially crafted SFTP packet is received from the server. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2019-3861	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH packets with a padding length value greater than the packet length are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2019-3862	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit status message and no payload are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2019-3863	A flaw was found in libssh2 before 1.8.1. A server could send a multiple keyboard interactive response messages whose total length are greater than unsigned char max characters. This value is used as an index to copy memory causing in an out of bounds memory write error.
CVE-2019-3877	A vulnerability was found in mod_auth_mellon before v0.14.2. An open redirect in the logout URL allows requests with backslashes to pass through by assuming that it is a relative URL, while the browsers silently convert backslash characters into forward slashes treating them as an absolute URL. This mismatch

	allows an attacker to bypass the redirect URL validation logic in apr_uri_parse function.
CVE-2019-3878	A vulnerability was found in mod_auth_mellon before v0.14.2. If Apache is configured as a reverse proxy and mod_auth_mellon is configured to only let through authenticated users (with the require valid-user directive), adding special HTTP headers that are normally used to start the special SAML ECP (non-browser based) can be used to bypass authentication.
CVE-2019-3880	A flaw was found in the way samba implemented an RPC endpoint emulating the Windows registry service API. An unprivileged attacker could use this flaw to create a new registry hive file anywhere they have unix permissions which could lead to creation of a new file in the Samba share. Versions before 4.8.11, 4.9.6 and 4.10.2 are vulnerable.
CVE-2019-3882	A flaw was found in the Linux kernel's vfio interface implementation that permits violation of the user's locked memory limit. If a device is bound to a vfio driver, such as vfio-pci, and the local attacker is administratively granted ownership of the device, it may cause a system memory exhaustion and thus a denial of service (DoS). Versions 3.10, 4.14 and 4.18 are vulnerable.
CVE-2019-3883	In 389-ds-base up to version 1.4.1.2, requests are handled by workers threads. Each sockets will be waited by the worker for at most 'ioblocktimeout' seconds. However this timeout applies only for un-encrypted requests. Connections using SSL/TLS are not taking this timeout into account during reads, and may hang longer. An unauthenticated attacker could repeatedly create hanging LDAP requests to hang all the workers, resulting in a Denial of Service.
CVE-2019-3885	A use-after-free flaw was found in pacemaker up to and including version 2.0.1 which could result in certain sensitive information to be leaked via the system logs.
CVE-2019-3890	It was discovered evolution-ews before 3.31.3 does not check the validity of SSL certificates. An attacker could abuse this flaw to get confidential information by tricking the user into connecting to a fake server without the user noticing the difference.
CVE-2019-3900	An infinite loop issue was found in the vhost_net kernel module in Linux Kernel up to and including v5.1-rc6, while handling incoming packets in handle_rx(). It could occur if one end sends packets faster than the other end can process them. A guest user, maybe remote one, could use this flaw to stall the vhost_net kernel thread, resulting in a DoS scenario.
CVE-2019-4014	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable

	to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force ID: 155892.
CVE-2019-4015	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-ForceID: 155893.
CVE-2019-4016	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-ForcelD: 155894.
CVE-2019-4030	IBM WebSphere Application Server 8.5 and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 155946.
CVE-2019-4057	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 could allow malicious user with access to the DB2 instance account to leverage a fenced execution process to execute arbitrary code as root. IBM X-Force ID: 156567.
CVE-2019-4094	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 binaries load shared libraries from an untrusted path potentially giving low privilege user full access to root by loading a malicious shared library. IBM X-Force ID: 158014.
CVE-2019-4101	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 10.1, 10.5, and 11.1 is vulnerable to a denial of service. Users that have both EXECUTE on PD_GET_DIAG_HIST and access to the diagnostic directory on the DB2 server can cause the instance to crash. IBM X-Force ID: 158091.
CVE-2019-4102	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 158092.
CVE-2019-4154	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force ID: 158519.
CVE-2019-4270	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Admin Console is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials

	disclosure within a trusted session. IBM X-Force ID: 160203.
CVE-2019-4271	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Admin console is vulnerable to a Client-side HTTP parameter pollution vulnerability. IBM X-Force ID: 160243.
CVE-2019-4279	IBM WebSphere Application Server 8.5 and 9.0 could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects from untrusted sources. IBM X-Force ID: 160445.
CVE-2019-4322	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 9.7, 10.1, 10.5, and 11.1 is vulnerable to a buffer overflow, which could allow an authenticated local attacker to execute arbitrary code on the system as root. IBM X-Force ID: 161202.
CVE-2019-4386	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 11.1 could allow an authenticated user to execute a function that would cause the server to crash. IBM X-Force ID: 162714.
CVE-2019-4441	IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0, and Liberty could allow a remote attacker to obtain sensitive information when a stack trace is returned in the browser. IBM X-Force ID: 163177.
CVE-2019-4442	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to traverse directories on the file system. An attacker could send a specially-crafted URL request to view arbitrary files on the system but not content. IBM X-Force ID: 163226.
CVE-2019-4477	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a user with access to audit logs to obtain sensitive information, caused by improper handling of command line options. IBM X-Force ID: 163997.
CVE-2019-4505	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 Network Deployment could allow a remote attacker to obtain sensitive information, caused by sending a specially-crafted URL. This can lead the attacker to view any file in a certain directory. IBM X-Force ID: 164364.
CVE-2019-5008	hw/sparc64/sun4u.c in QEMU 3.1.50 is vulnerable to a NULL pointer dereference, which allows the attacker to cause a denial of service via a device driver.
CVE-2019-5010	An exploitable denial-of-service vulnerability exists in the X509 certificate parser of Python.org Python 2.7.11 / 3.6.6. A specially crafted X509 certificate can cause a NULL pointer dereference, resulting in a denial of service. An attacker can initiate or accept

	TLS connections using crafted certificates to trigger this vulnerability.
CVE-2019-5094	An exploitable code execution vulnerability exists in the quota file functionality of E2fsprogs 1.45.3. A specially crafted ext4 partition can cause an out-of-bounds write on the heap, resulting in code execution. An attacker can corrupt a partition to trigger this vulnerability.
CVE-2019-5188	A code execution vulnerability exists in the directory rehashing functionality of E2fsprogs e2fsck 1.45.4. A specially crafted ext4 directory can cause an out-of-bounds write on the stack, resulting in code execution. An attacker can corrupt a partition to trigger this vulnerability.
CVE-2019-5435	An integer overflow in curl's URL API results in a buffer overflow in libcurl 7.62.0 to and including 7.64.1.
CVE-2019-5436	A heap buffer overflow in the TFTP receiving code allows for DoS or arbitrary code execution in libcurl versions 7.19.4 through 7.64.1.
CVE-2019-5481	Double-free vulnerability in the FTP-kerberos code in cURL 7.52.0 to 7.65.3.
CVE-2019-5482	Heap buffer overflow in the TFTP protocol handler in cURL 7.19.4 to 7.65.3.
CVE-2019-5489	The mincore() implementation in mm/mincore.c in the Linux kernel through 4.19.13 allowed local attackers to observe page cache access patterns of other processes on the same system, potentially allowing sniffing of secret information. (Fixing this affects the output of the fincore program.) Limited remote exploitation may be possible, as demonstrated by latency differences in accessing public files from an Apache HTTP Server.
CVE-2019-5527	ESXi, Workstation, Fusion, VMRC and Horizon Client contain a use-after-free vulnerability in the virtual sound device. VMware has evaluated the severity of this issue to be in the Important severity range with a maximum CVSSv3 base score of 8.5.
CVE-2019-5544	OpenSLP as used in ESXi and the Horizon DaaS appliances has a heap overwrite issue. VMware has evaluated the severity of this issue to be in the Critical severity range with a maximum CVSSv3 base score of 9.8.
CVE-2019-5736	runc through 1.0-rc6, as used in Docker before 18.09.2 and other products, allows attackers to overwrite the host runc binary (and consequently obtain host root access) by leveraging the ability to execute a command as root within one of these types of containers: (1) a new container with an attacker-controlled image, or (2) an existing container, to which the attacker previously had write access, that can be attached with

	docker exec. This occurs because of file-descriptor mishandling, related to /proc/self/exe.
CVE-2019-5754	Implementation error in QUIC Networking in Google Chrome prior to 72.0.3626.81 allowed an attacker running or able to cause use of a proxy server to obtain cleartext of transport encryption via malicious network proxy.
CVE-2019-5755	Incorrect handling of negative zero in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page.
CVE-2019-5756	Inappropriate memory management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.
CVE-2019-5757	An incorrect object type assumption in SVG in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2019-5758	Incorrect object lifecycle management in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5759	Incorrect lifetime handling in HTML select elements in Google Chrome on Android and Mac prior to 72.0.3626.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2019-5760	Insufficient checks of pointer validity in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5761	Incorrect object lifecycle management in SwiftShader in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5762	Inappropriate memory management when caching in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.
CVE-2019-5763	Failure to check error conditions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5764	Incorrect pointer management in WebRTC in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5765	An exposed debugging endpoint in the browser in Google Chrome on Android prior to 72.0.3626.81

	allowed a local attacker to obtain potentially sensitive information from process memory via a crafted Intent.
CVE-2019-5766	Incorrect handling of origin taint checking in Canvas in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-5767	Insufficient protection of permission UI in WebAPKs in Google Chrome on Android prior to 72.0.3626.81 allowed an attacker who convinced the user to install a malicious application to access privacy/security sensitive web APIs via a crafted APK.
CVE-2019-5768	DevTools API not correctly gating on extension capability in DevTools in Google Chrome prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to read local files via a crafted Chrome Extension.
CVE-2019-5769	Incorrect handling of invalid end character position when front rendering in Blink in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5770	Insufficient input validation in WebGL in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2019-5771	An incorrect JIT of GLSL shaders in SwiftShader in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2019-5772	Sharing of objects over calls into JavaScript runtime in PDFium in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5773	Insufficient origin validation in IndexedDB in Google Chrome prior to 72.0.3626.81 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page.
CVE-2019-5774	Omission of the .desktop filetype from the Safe Browsing checklist in SafeBrowsing in Google Chrome on Linux prior to 72.0.3626.81 allowed an attacker who convinced a user to download a .desktop file to execute arbitrary code via a downloaded .desktop file.
CVE-2019-5775	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2019-5776	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.

CVE-2019-5777	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2019-5778	A missing case for handling special schemes in permission request checks in Extensions in Google Chrome prior to 72.0.3626.81 allowed an attacker who convinced a user to install a malicious extension to bypass extension permission checks for privileged pages via a crafted Chrome Extension.
CVE-2019-5779	Insufficient policy validation in ServiceWorker in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2019-5780	Insufficient restrictions on what can be done with Apple Events in Google Chrome on macOS prior to 72.0.3626.81 allowed a local attacker to execute JavaScript via Apple Events.
CVE-2019-5781	Incorrect handling of a confusable character in Omnibox in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2019-5782	Incorrect optimization assumptions in V8 in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2019-5783	Missing URI encoding of untrusted input in DevTools in Google Chrome prior to 72.0.3626.81 allowed a remote attacker to perform a Dangling Markup Injection attack via a crafted HTML page.
CVE-2019-5784	Incorrect handling of deferred code in V8 in Google Chrome prior to 72.0.3626.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5786	Object lifetime issue in Blink in Google Chrome prior to 72.0.3626.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2019-5787	Use-after-garbage-collection in Blink in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5788	An integer overflow that leads to a use-after-free in Blink Storage in Google Chrome on Linux prior to 73.0.3683.75 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page.
CVE-2019-5789	An integer overflow that leads to a use-after-free in WebMIDI in Google Chrome on Windows prior to

	73.0.3683.75 allowed a remote attacker who had compromised the renderer process to execute arbitrary code via a crafted HTML page.
CVE-2019-5790	An integer overflow leading to an incorrect capacity of a buffer in JavaScript in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2019-5791	Inappropriate optimization in V8 in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2019-5792	Integer overflow in PDFium in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially perform out of bounds memory access via a crafted PDF file.
CVE-2019-5793	Insufficient policy enforcement in extensions in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to initiate the extensions installation user interface via a crafted HTML page.
CVE-2019-5794	Incorrect handling of cancelled requests in Navigation in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2019-5795	Integer overflow in PDFium in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially perform out of bounds memory access via a crafted PDF file.
CVE-2019-5796	Data race in extensions guest view in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5798	Lack of correct bounds checking in Skia in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2019-5799	Incorrect inheritance of a new document's policy in Content Security Policy in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2019-5800	Insufficient policy enforcement in Blink in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2019-5802	Incorrect handling of download origins in Navigation in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.

CVE-2019-5803	Insufficient policy enforcement in Content Security Policy in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2019-5805	Use-after-free in PDFium in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5806	Integer overflow in ANGLE in Google Chrome on Windows prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5807	Object lifetime issue in V8 in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5808	Use after free in Blink in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5809	Use after free in file chooser in Google Chrome prior to 74.0.3729.108 allowed a remote attacker who had compromised the renderer process to perform privilege escalation via a crafted HTML page.
CVE-2019-5810	Information leak in autofill in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-5811	Incorrect handling of CORS in ServiceWorker in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass same origin policy via a crafted HTML page.
CVE-2019-5813	Use after free in V8 in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5814	Insufficient policy enforcement in Blink in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-5815	Type confusion in xsltNumberFormatGetMultipleLevel prior to libxslt 1.1.33 could allow attackers to potentially exploit heap corruption via crafted XML data.
CVE-2019-5818	Uninitialized data in media in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted video file.
CVE-2019-5819	Insufficient data validation in developer tools in Google Chrome on OS X prior to 74.0.3729.108 allowed a local attacker to execute arbitrary code via a crafted string copied to clipboard.

CVE-2019-5820	Integer overflow in PDFium in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5821	Integer overflow in PDFium in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5822	Inappropriate implementation in Blink in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass same origin policy via a crafted HTML page.
CVE-2019-5823	Insufficient policy enforcement in service workers in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2019-5824	Parameter passing error in media in Google Chrome prior to 74.0.3729.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5825	Out of bounds write in JavaScript in Google Chrome prior to 73.0.3683.86 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5826	Use after free in IndexedDB in Google Chrome prior to 73.0.3683.86 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5827	Integer overflow in SQLite via WebSQL in Google Chrome prior to 74.0.3729.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5828	Object lifecycle issue in ServiceWorker in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2019-5829	Integer overflow in download manager in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2019-5830	Insufficient policy enforcement in CORS in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-5831	Object lifecycle issue in V8 in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5832	Insufficient policy enforcement in XMLHttpRequest in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page.

CVE-2019-5833	Incorrect dialog box scoping in browser in Google Chrome on Android prior to 75.0.3770.80 allowed a remote attacker to display misleading security UI via a crafted HTML page.
CVE-2019-5835	Object lifecycle issue in SwiftShader in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2019-5836	Heap buffer overflow in ANGLE in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5837	Resource size information leakage in Blink in Google Chrome prior to 75.0.3770.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-5838	Insufficient policy enforcement in extensions API in Google Chrome prior to 75.0.3770.80 allowed an attacker who convinced a user to install a malicious extension to bypass restrictions on file URIs via a crafted Chrome Extension.
CVE-2019-5839	Excessive data validation in URL parser in Google Chrome prior to 75.0.3770.80 allowed a remote attacker who convinced a user to input a URL to bypass website URL validation via a crafted URL.
CVE-2019-5840	Incorrect security UI in popup blocker in Google Chrome on iOS prior to 75.0.3770.80 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2019-5842	Use after free in Blink in Google Chrome prior to 75.0.3770.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5844	Out of bounds access in SwiftShader in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5845	Out of bounds access in SwiftShader in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5846	Out of bounds access in SwiftShader in Google Chrome prior to 73.0.3683.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5847	Inappropriate implementation in JavaScript in Google Chrome prior to 75.0.3770.142 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5848	Incorrect font handling in autofill in Google Chrome prior to 75.0.3770.142 allowed a remote attacker to obtain

	potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-5850	Use after free in offline mode in Google Chrome prior to 76.0.3809.87 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2019-5851	Use after free in WebAudio in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5852	Inappropriate implementation in JavaScript in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-5853	Inappropriate implementation in JavaScript in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5854	Integer overflow in PDFium in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5855	Integer overflow in PDFium in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5856	Insufficient policy enforcement in storage in Google Chrome prior to 76.0.3809.87 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.
CVE-2019-5857	Inappropriate implementation in JavaScript in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2019-5858	Incorrect security UI in MacOS services integration in Google Chrome on OS X prior to 76.0.3809.87 allowed a local attacker to execute arbitrary code via a crafted HTML page.
CVE-2019-5859	Insufficient filtering in URI schemes in Google Chrome on Windows prior to 76.0.3809.87 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2019-5860	Use after free in PDFium in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5861	Insufficient data validation in Blink in Google Chrome prior to 76.0.3809.87 allowed a remote attacker to bypass anti-clickjacking policy via a crafted HTML page.
CVE-2019-5862	Insufficient data validation in AppCache in Google Chrome prior to 76.0.3809.87 allowed a remote attacker

	who had compromised the renderer process to bypass site isolation via a crafted HTML page.
CVE-2019-5864	Insufficient data validation in CORS in Google Chrome prior to 76.0.3809.87 allowed an attacker who convinced a user to install a malicious extension to bypass content security policy via a crafted Chrome Extension.
CVE-2019-5865	Insufficient policy enforcement in navigations in Google Chrome prior to 76.0.3809.87 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.
CVE-2019-5867	Out of bounds read in JavaScript in Google Chrome prior to 76.0.3809.100 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5868	Use after free in PDFium in Google Chrome prior to 76.0.3809.100 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2019-5869	Use after free in Blink in Google Chrome prior to 76.0.3809.132 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5870	Use after free in media in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2019-5871	Heap buffer overflow in Skia in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5872	Use after free in Mojo in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5874	Insufficient filtering in URI schemes in Google Chrome on Windows prior to 77.0.3865.75 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2019-5875	Insufficient data validation in downloads in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2019-5876	Use after free in media in Google Chrome on Android prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5877	Out of bounds memory access in JavaScript in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2019-5878	Use after free in V8 in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2019-5879	Insufficient policy enforcement in extensions in Google Chrome prior to 77.0.3865.75 allowed an attacker who convinced a user to install a malicious extension to read local files via a crafted Chrome Extension.
CVE-2019-5880	Insufficient policy enforcement in Blink in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2019-5881	Out of bounds read in SwiftShader in Google Chrome prior to 77.0.3865.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2019-5953	Buffer overflow in GNU Wget 1.20.1 and earlier allows remote attackers to cause a denial-of-service (DoS) or may execute an arbitrary code via unspecified vectors.
CVE-2019-6109	An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.
CVE-2019-6111	An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).
CVE-2019-6116	In Artifex Ghostscript through 9.26, ephemeral or transient procedures can allow access to system operators, leading to remote code execution.
CVE-2019-6133	In PolicyKit (aka polkit) 0.115, the "start time" protection mechanism can be bypassed because fork() is not atomic, and therefore authorization decisions are improperly cached. This is related to lack of uid checking in polkitbackend/polkitbackendinteractiveauthority.c.
CVE-2019-6237	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12.

	Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-6251	WebKitGTK and WPE WebKit prior to version 2.24.1 are vulnerable to address bar spoofing upon certain JavaScript redirections. An attacker could cause malicious web content to be displayed as if for a trusted URI. This is similar to the CVE-2018-8383 issue in Microsoft Edge.
CVE-2019-6454	An issue was discovered in sd-bus in systemd 239. bus_process_object() in libsystemd/sd-bus/bus-objects.c allocates a variable-length stack buffer for temporarily storing the object path of incoming D-Bus messages. An unprivileged local user can exploit this by sending a specially crafted message to PID1, causing the stack pointer to jump over the stack guard pages into an unmapped memory region and trigger a denial of service (systemd PID1 crash and kernel panic).
CVE-2019-6465	Controls for zone transfers may not be properly applied to Dynamically Loadable Zones (DLZs) if the zones are writable Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.5-P2, 9.12.0 -> 9.12.3-P2, and versions 9.9.3-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2019-6465.
CVE-2019-6470	There had existed in one of the ISC BIND libraries a bug in a function that was used by dhcpcd when operating in DHCPv6 mode. There was also a bug in dhcpcd relating to the use of this function per its documentation, but the bug in the library function prevented this from causing any harm. All releases of dhcpcd from ISC contain copies of this, and other, BIND libraries in combinations that have been tested prior to release and are known to not present issues like this. Some third-party packagers of ISC software have modified the dhcpcd source, BIND source, or version matchup in ways that create the crash potential. Based on reports available to ISC, the crash probability is large and no analysis has been done on how, or even if, the probability can be manipulated by an attacker. Affects: Builds of dhcpcd versions prior to version 4.4.1 when using BIND versions 9.11.2 or later, or BIND versions with specific bug fixes backported to them. ISC does not have access to comprehensive version lists for all repackagings of dhcpcd that are vulnerable. In particular, builds from other vendors may also be affected. Operators are advised to consult their vendor documentation.
CVE-2019-6477	With pipelining enabled each incoming query on a TCP connection requires a similar resource allocation to a

	query received via UDP or via TCP without pipelining enabled. A client using a TCP-pipelined connection to a server could consume more resources than the server has been provisioned to handle. When a TCP connection with a large number of pipelined queries is closed, the load on the server releasing these multiple resources can cause it to become unresponsive, even for queries that can be answered authoritatively or from cache. (This is most likely to be perceived as an intermittent server problem).
CVE-2019-6486	Go before 1.10.8 and 1.11.x before 1.11.5 mishandles P-521 and P-384 elliptic curves, which allows attackers to cause a denial of service (CPU consumption) or possibly conduct ECDH private key recovery attacks.
CVE-2019-6974	In the Linux kernel before 4.20.8, kvm_ioctl_create_device in virt/kvm/kvm_main.c mishandles reference counting because of a race condition, leading to a use-after-free.
CVE-2019-6978	The GD Graphics Library (aka LibGD) 2.2.5 has a double free in the gdImage*Ptr() functions in gd_gif_out.c, gd_jpeg.c, and gd_wbmp.c. NOTE: PHP is unaffected.
CVE-2019-7090	Flash Player Desktop Runtime versions 32.0.0.114 and earlier, Flash Player for Google Chrome versions 32.0.0.114 and earlier, and Flash Player for Microsoft Edge and Internet Explorer 11 versions 32.0.0.114 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2019-7096	Adobe Flash Player versions 32.0.0.156 and earlier, 32.0.0.156 and earlier, and 32.0.0.156 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2019-7108	Adobe Flash Player versions 32.0.0.156 and earlier, 32.0.0.156 and earlier, and 32.0.0.156 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure .
CVE-2019-7149	A heap-based buffer over-read was discovered in the function read_srclines in dwarf_getsrclines.c in libdw in elfutils 0.175. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by eu-nm.
CVE-2019-7150	An issue was discovered in elfutils 0.175. A segmentation fault can occur in the function elf64_xlatetom in libelf/elf32_xlatetom.c, due to dwfl_segment_report_module not checking whether the dyn data read from a core file is truncated. A crafted input can cause a program crash, leading to denial-of-service, as demonstrated by eu-stack.

CVE-2019-7175	In ImageMagick before 7.0.8-25, some memory leaks exist in DecodeImage in coders/pcd.c.
CVE-2019-7221	The KVM implementation in the Linux kernel through 4.20.5 has a Use-after-Free.
CVE-2019-7222	The KVM implementation in the Linux kernel through 4.20.5 has an Information Leak.
CVE-2019-7308	kernel/bpf/verifier.c in the Linux kernel before 4.20.6 performs undesirable out-of-bounds speculation on pointer arithmetic in various cases, including cases of different branches with different state or limits to sanitize, leading to side-channel attacks.
CVE-2019-7310	In Poppler 0.73.0, a heap-based buffer over-read (due to an integer signedness error in the XRef::getEntry function in XRef.cc) allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PDF document, as demonstrated by pdftocairo.
CVE-2019-7317	png_image_free in png.c in libpng 1.6.x before 1.6.37 has a use-after-free because png_image_free_function is called under png_safe_execute.
CVE-2019-7397	In ImageMagick before 7.0.8-25 and GraphicsMagick through 1.3.31, several memory leaks exist in WritePDFImage in coders/pdf.c.
CVE-2019-7398	In ImageMagick before 7.0.8-25, a memory leak exists in WriteDIBImage in coders/dib.c.
CVE-2019-7524	In Dovecot before 2.2.36.3 and 2.3.x before 2.3.5.1, a local attacker can cause a buffer overflow in the indexer-worker process, which can be used to elevate to root. This occurs because of missing checks in the fts and pop3-uidl components.
CVE-2019-7572	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a buffer over-read in IMA_ADPCM_nibble in audio/SDL_wave.c.
CVE-2019-7573	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in InitMS_ADPCM in audio/SDL_wave.c (inside the wNumCoef loop).
CVE-2019-7574	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in IMA_ADPCM_decode in audio/SDL_wave.c.
CVE-2019-7575	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer overflow in MS_ADPCM_decode in audio/SDL_wave.c.
CVE-2019-7576	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in InitMS_ADPCM in audio/SDL_wave.c (outside the wNumCoef loop).

CVE-2019-7577	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a buffer over-read in <code>SDL_LoadWAV_RW</code> in <code>audio/SDL_wave.c</code> .
CVE-2019-7578	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in <code>InitIMA_ADPCM</code> in <code>audio/SDL_wave.c</code> .
CVE-2019-7608	Kibana versions before 5.6.15 and 6.6.1 had a cross-site scripting (XSS) vulnerability that could allow an attacker to obtain sensitive information from or perform destructive actions on behalf of other Kibana users.
CVE-2019-7609	Kibana versions before 5.6.15 and 6.6.1 contain an arbitrary code execution flaw in the Timelion visualizer. An attacker with access to the Timelion application could send a request that will attempt to execute javascript code. This could possibly lead to an attacker executing arbitrary commands with permissions of the Kibana process on the host system.
CVE-2019-7610	Kibana versions before 6.6.1 contain an arbitrary code execution flaw in the security audit logger. If a Kibana instance has the setting <code>xpack.security.audit.enabled</code> set to true, an attacker could send a request that will attempt to execute javascript code. This could possibly lead to an attacker executing arbitrary commands with permissions of the Kibana process on the host system.
CVE-2019-7614	A race condition flaw was found in the response headers Elasticsearch versions before 7.2.1 and 6.8.2 returns to a request. On a system with multiple users submitting requests, it could be possible for an attacker to gain access to response header containing sensitive data from another user.
CVE-2019-7616	Kibana versions before 6.8.2 and 7.2.1 contain a server side request forgery (SSRF) flaw in the graphite integration for Timelion visualizer. An attacker with administrative Kibana access could set the <code>timelion:graphite.url</code> configuration option to an arbitrary URL. This could possibly lead to an attacker accessing external URL resources as the Kibana process on the host system.
CVE-2019-7619	Elasticsearch versions 7.0.0-7.3.2 and 6.7.0-6.8.3 contain a username disclosure flaw was found in the API Key service. An unauthenticated attacker could send a specially crafted request and determine if a username exists in the Elasticsearch native realm.
CVE-2019-7621	Kibana versions before 6.8.6 and 7.5.1 contain a cross site scripting (XSS) flaw in the coordinate and region map visualizations. An attacker with the ability to create coordinate map visualizations could create a malicious visualization. If another Kibana user views that visualization or a dashboard containing

	the visualization it could execute JavaScript in the victim's browser.
CVE-2019-7635	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in Blit1to4 in video/SDL_blit_1.c.
CVE-2019-7636	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in SDL_GetRGB in video/SDL_pixels.c.
CVE-2019-7637	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer overflow in SDL_FillRect in video/SDL_surface.c.
CVE-2019-7638	SDL (Simple DirectMedia Layer) through 1.2.15 and 2.x through 2.0.9 has a heap-based buffer over-read in Map1toN in video/SDL_pixels.c.
CVE-2019-7652	TheHive Project UnshortenLink analyzer before 1.1, included in Cortex-Analyzers before 1.15.2, has SSRF. To exploit the vulnerability, an attacker must create a new analysis, select URL for Data Type, and provide an SSRF payload like "http://127.0.0.1:22" in the Data parameter. The result can be seen in the main dashboard. Thus, it is possible to do port scans on localhost and intranet hosts.
CVE-2019-7664	In elfutils 0.175, a negative-sized memcpy is attempted in elf_cvt_note in libelf/note_xlate.h because of an incorrect overflow check. Crafted elf input causes a segmentation fault, leading to denial of service (program crash).
CVE-2019-7665	In elfutils 0.175, a heap-based buffer over-read was discovered in the function elf32_xlatetom in elf32_xlatetom.c in libelf. A crafted ELF input can cause a segmentation fault leading to denial of service (program crash) because ebl_core_note does not reject malformed core file notes.
CVE-2019-7837	Adobe Flash Player versions 32.0.0.171 and earlier, 32.0.0.171 and earlier, and 32.0.0.171 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2019-7845	Adobe Flash Player versions 32.0.0.192 and earlier, 32.0.0.192 and earlier, and 32.0.0.192 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2019-8069	Adobe Flash Player 32.0.0.238 and earlier versions, 32.0.0.207 and earlier versions have a Same Origin Method Execution vulnerability. Successful exploitation could lead to Arbitrary Code Execution in the context of the current user.
CVE-2019-8070	Adobe Flash Player 32.0.0.238 and earlier versions, 32.0.0.207 and earlier versions have a Use after free vulnerability. Successful exploitation could lead to

	Arbitrary Code Execution in the context of the current user.
CVE-2019-8075	Adobe Flash Player version 32.0.0.192 and earlier versions have a Same Origin Policy Bypass vulnerability. Successful exploitation could lead to Information Disclosure in the context of the current user.
CVE-2019-8308	Flatpak before 1.0.7, and 1.1.x and 1.2.x before 1.2.3, exposes /proc in the apply_extra script sandbox, which allows attackers to modify a host-side executable file.
CVE-2019-8322	An issue was discovered in RubyGems 2.6 and later through 3.0.2. The gem owner command outputs the contents of the API response directly to stdout. Therefore, if the response is crafted, escape sequence injection may occur.
CVE-2019-8323	An issue was discovered in RubyGems 2.6 and later through 3.0.2. Gem::GemcutterUtilities#with_response may output the API response to stdout as it is. Therefore, if the API side modifies the response, escape sequence injection may occur.
CVE-2019-8324	An issue was discovered in RubyGems 2.6 and later through 3.0.2. A crafted gem with a multi-line name is not handled correctly. Therefore, an attacker could inject arbitrary code to the stub line of gemspec, which is eval-ed by code in ensure_loadable_spec during the preinstall check.
CVE-2019-8325	An issue was discovered in RubyGems 2.6 and later through 3.0.2. Since Gem::CommandManager#run calls alert_error without escaping, escape sequence injection is possible. (There are many ways to cause an error.)
CVE-2019-8331	In Bootstrap before 3.4.1 and 4.3.x before 4.3.1, XSS is possible in the tooltip or popover data-template attribute.
CVE-2019-8379	An issue was discovered in AdvanceCOMP through 2.1. A NULL pointer dereference exists in the function be_uint32_read() located in endianrw.h. It can be triggered by sending a crafted file to a binary. It allows an attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact when a victim opens a specially crafted file.
CVE-2019-8383	An issue was discovered in AdvanceCOMP through 2.1. An invalid memory address occurs in the function adv_png_unfilter_8 in lib/png.c. It can be triggered by sending a crafted file to a binary. It allows an attacker to cause a Denial of Service (Segmentation fault) or possibly have unspecified other impact when a victim opens a specially crafted file.
CVE-2019-8506	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 12.2,

	tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8524	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8535	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8536	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8544	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8551	A logic issue was addressed with improved validation. This issue is fixed in iOS 12.2, tvOS 12.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to universal cross site scripting.
CVE-2019-8558	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8559	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8563	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.2, tvOS 12.2, watchOS 5.2, Safari 12.1, iTunes 12.9.4 for Windows, iCloud for Windows 7.11.

	Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8571	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8583	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8584	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8586	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8587	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8594	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8595	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8596	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.

CVE-2019-8597	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8601	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8607	An out-of-bounds read was addressed with improved input validation. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may result in the disclosure of process memory.
CVE-2019-8608	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8609	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8610	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8611	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8615	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8619	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS

	12.3, macOS Mojave 10.14.5, tvOS 12.3, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8622	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8623	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.3, macOS Mojave 10.14.5, tvOS 12.3, watchOS 5.2.1, Safari 12.1.1, iTunes for Windows 12.9.5, iCloud for Windows 7.12. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8625	A logic issue was addressed with improved state management. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to universal cross site scripting.
CVE-2019-8644	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8649	A logic issue existed in the handling of synchronous page loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting.
CVE-2019-8658	A logic issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting.
CVE-2019-8666	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.

CVE-2019-8669	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8671	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8672	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8673	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8674	A logic issue was addressed with improved state management. This issue is fixed in iOS 13, Safari 13. Processing maliciously crafted web content may lead to universal cross site scripting.
CVE-2019-8675	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6, Security Update 2019-004 High Sierra, Security Update 2019-004 Sierra. An attacker in a privileged network position may be able to execute arbitrary code.
CVE-2019-8676	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8677	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing

	maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8678	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8679	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8680	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8681	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8683	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8684	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8686	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing

	maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8687	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8688	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8689	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, watchOS 5.3, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8690	A logic issue existed in the handling of document loads. This issue was addressed with improved state management. This issue is fixed in iOS 12.4, macOS Mojave 10.14.6, tvOS 12.4, Safari 12.1.2, iTunes for Windows 12.9.6, iCloud for Windows 7.13, iCloud for Windows 10.6. Processing maliciously crafted web content may lead to universal cross site scripting.
CVE-2019-8696	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in macOS Mojave 10.14.6, Security Update 2019-004 High Sierra, Security Update 2019-004 Sierra. An attacker in a privileged network position may be able to execute arbitrary code.
CVE-2019-8707	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8710	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8719	A logic issue was addressed with improved state management. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud

	for Windows 7.14. Processing maliciously crafted web content may lead to universal cross site scripting.
CVE-2019-8720	** 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-2019-8726	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8733	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8735	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8743	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in watchOS 6.1. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8763	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.1 and iPadOS 13.1, tvOS 13, Safari 13.0.1, iTunes for Windows 12.10.1, iCloud for Windows 10.7, iCloud for Windows 7.14. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8764	A logic issue was addressed with improved state management. This issue is fixed in watchOS 6.1. Processing maliciously crafted web content may lead to universal cross site scripting.
CVE-2019-8765	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in watchOS 6.1. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8766	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in watchOS 6.1, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution.

CVE-2019-8768	"Clear History and Website Data" did not clear the history. The issue was addressed with improved data deletion. This issue is fixed in macOS Catalina 10.15. A user may be unable to delete browsing history items.
CVE-2019-8769	An issue existed in the drawing of web page elements. The issue was addressed with improved logic. This issue is fixed in iOS 13.1 and iPadOS 13.1, macOS Catalina 10.15. Visiting a maliciously crafted website may reveal browsing history.
CVE-2019-8771	This issue was addressed with improved iframe sandbox enforcement. This issue is fixed in Safari 13.0.1, iOS 13. Maliciously crafted web content may violate iframe sandboxing policy.
CVE-2019-8782	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8783	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8808	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8811	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8812	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8813	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0. Processing maliciously crafted web content may lead to universal cross site scripting.

CVE-2019-8814	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8815	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8816	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8819	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8820	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, watchOS 6.1, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8821	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8822	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8823	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.2 and iPadOS 13.2, tvOS 13.2, Safari 13.0.3, iTunes for Windows 12.10.2, iCloud for Windows 11.0, iCloud for Windows 7.15. Processing maliciously crafted web content may lead to arbitrary code execution.

CVE-2019-8835	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13.3, iCloud for Windows 10.9, iOS 13.3 and iPadOS 13.3, Safari 13.0.4, iTunes 12.10.3 for Windows, iCloud for Windows 7.16. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8844	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 13.3, watchOS 6.1.1, iCloud for Windows 10.9, iOS 13.3 and iPadOS 13.3, Safari 13.0.4, iTunes 12.10.3 for Windows, iCloud for Windows 7.16. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8846	A use after free issue was addressed with improved memory management. This issue is fixed in tvOS 13.3, iCloud for Windows 10.9, iOS 13.3 and iPadOS 13.3, Safari 13.0.4, iTunes 12.10.3 for Windows, iCloud for Windows 7.16. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2019-8912	In the Linux kernel through 4.20.11, af_alg_release() in crypto/af_alg.c neglects to set a NULL value for a certain structure member, which leads to a use-after-free in sockfs_setattr.
CVE-2019-8980	A memory leak in the kernel_read_file function in fs/exec.c in the Linux kernel through 4.20.11 allows attackers to cause a denial of service (memory consumption) by triggering vfs_read failures.
CVE-2019-9169	In the GNU C Library (aka glibc or libc6) through 2.29, proceed_next_node in posix/regexec.c has a heap-based buffer over-read via an attempted case-insensitive regular-expression match.
CVE-2019-9200	A heap-based buffer underwrite exists in ImageStream::getLine() located at Stream.cc in Poppler 0.74.0 that can (for example) be triggered by sending a crafted PDF file to the pdfimages binary. It allows an attacker to cause Denial of Service (Segmentation fault) or possibly have unspecified other impact.
CVE-2019-9210	In AdvanceCOMP 2.1, png_compress in pngex.cc in advpng has an integer overflow upon encountering an invalid PNG size, which results in an attempted memcpy to write into a buffer that is too small. (There is also a heap-based buffer over-read.)
CVE-2019-9213	In the Linux kernel before 4.20.14, expand_downwards in mm/mmap.c lacks a check for the mmap minimum address, which makes it easier for attackers to exploit kernel NULL pointer dereferences on non-SMAP platforms. This is related to a capability check for the wrong task.
CVE-2019-9232	In libvpx, there is a possible out of bounds read due to a missing bounds check. This could lead to

	remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-122675483
CVE-2019-9278	In libexif, there is a possible out of bounds write due to an integer overflow. This could lead to remote escalation of privilege in the media content provider with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-112537774
CVE-2019-9433	In libvpx, there is a possible information disclosure due to improper input validation. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-10Android ID: A-80479354
CVE-2019-9445	In the Android kernel in F2FS driver there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with system execution privileges needed. User interaction is not needed for exploitation.
CVE-2019-9500	The Broadcom brcmfmac WiFi driver prior to commit 1b5e2423164b3670e8bc9174e4762d297990deff is vulnerable to a heap buffer overflow. If the Wake-up on Wireless LAN functionality is configured, a malicious event frame can be constructed to trigger an heap buffer overflow in the brcmf_wowl_nd_results function. This vulnerability can be exploited with compromised chipsets to compromise the host, or when used in combination with CVE-2019-9503, can be used remotely. In the worst case scenario, by sending specially-crafted WiFi packets, a remote, unauthenticated attacker may be able to execute arbitrary code on a vulnerable system. More typically, this vulnerability will result in denial-of-service conditions.
CVE-2019-9511	Some HTTP/2 implementations are vulnerable to window size manipulation and stream prioritization manipulation, potentially leading to a denial of service. The attacker requests a large amount of data from a specified resource over multiple streams. They manipulate window size and stream priority to force the server to queue the data in 1-byte chunks. Depending on how efficiently this data is queued, this can consume excess CPU, memory, or both.
CVE-2019-9512	Some HTTP/2 implementations are vulnerable to ping floods, potentially leading to a denial of service. The attacker sends continual pings to an HTTP/2 peer, causing the peer to build an internal queue of responses. Depending on how efficiently this data is

	queued, this can consume excess CPU, memory, or both.
CVE-2019-9513	Some HTTP/2 implementations are vulnerable to resource loops, potentially leading to a denial of service. The attacker creates multiple request streams and continually shuffles the priority of the streams in a way that causes substantial churn to the priority tree. This can consume excess CPU.
CVE-2019-9514	Some HTTP/2 implementations are vulnerable to a reset flood, potentially leading to a denial of service. The attacker opens a number of streams and sends an invalid request over each stream that should solicit a stream of RST_STREAM frames from the peer. Depending on how the peer queues the RST_STREAM frames, this can consume excess memory, CPU, or both.
CVE-2019-9516	Some HTTP/2 implementations are vulnerable to a header leak, potentially leading to a denial of service. The attacker sends a stream of headers with a 0-length header name and 0-length header value, optionally Huffman encoded into 1-byte or greater headers. Some implementations allocate memory for these headers and keep the allocation alive until the session dies. This can consume excess memory.
CVE-2019-9517	Some HTTP/2 implementations are vulnerable to unconstrained interal data buffering, potentially leading to a denial of service. The attacker opens the HTTP/2 window so the peer can send without constraint; however, they leave the TCP window closed so the peer cannot actually write (many of) the bytes on the wire. The attacker then sends a stream of requests for a large response object. Depending on how the servers queue the responses, this can consume excess memory, CPU, or both.
CVE-2019-9631	Poppler 0.74.0 has a heap-based buffer over-read in the CairoRescaleBox.cc downsample_row_box_filter function.
CVE-2019-9636	Python 2.7.x through 2.7.16 and 3.x through 3.7.2 is affected by: Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization. The impact is: Information disclosure (credentials, cookies, etc. that are cached against a given hostname). The components are: urllib.parse.urlsplit, urllib.parse.urlparse. The attack vector is: A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly. This is fixed in: v2.7.17, v2.7.17rc1, v2.7.18, v2.7.18rc1; v3.5.10, v3.5.10rc1, v3.5.7, v3.5.8, v3.5.8rc1, v3.5.8rc2, v3.5.9; v3.6.10, v3.6.10rc1, v3.6.11, v3.6.11rc1, v3.6.12, v3.6.9, v3.6.9rc1;

	v3.7.3, v3.7.3rc1, v3.7.4, v3.7.4rc1, v3.7.4rc2, v3.7.5, v3.7.5rc1, v3.7.6, v3.7.6rc1, v3.7.7, v3.7.7rc1, v3.7.8, v3.7.8rc1, v3.7.9.
CVE-2019-9740	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the query string after a ? character) followed by an HTTP header or a Redis command. This is fixed in: v2.7.17, v2.7.17rc1, v2.7.18, v2.7.18rc1; v3.5.10, v3.5.10rc1, v3.5.8, v3.5.8rc1, v3.5.8rc2, v3.5.9; v3.6.10, v3.6.10rc1, v3.6.11, v3.6.11rc1, v3.6.12, v3.6.9, v3.6.9rc1; v3.7.4, v3.7.4rc1, v3.7.4rc2, v3.7.5, v3.7.5rc1, v3.7.6, v3.7.6rc1, v3.7.7, v3.7.7rc1, v3.7.8, v3.7.8rc1, v3.7.9.
CVE-2019-9755	An integer underflow issue exists in ntfs-3g 2017.3.23. A local attacker could potentially exploit this by running /bin/ntfs-3g with specially crafted arguments from a specially crafted directory to cause a heap buffer overflow, resulting in a crash or the ability to execute arbitrary code. In installations where /bin/ntfs-3g is a setuid-root binary, this could lead to a local escalation of privileges.
CVE-2019-9788	Mozilla developers and community members reported memory safety bugs present in Firefox 65, Firefox ESR 60.5, and Thunderbird 60.5. 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 < 60.6, Firefox ESR < 60.6, and Firefox < 66.
CVE-2019-9790	A use-after-free vulnerability can occur when a raw pointer to a DOM element on a page is obtained using JavaScript and the element is then removed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.
CVE-2019-9791	The type inference system allows the compilation of functions that can cause type confusions between arbitrary objects when compiled through the IonMonkey just-in-time (JIT) compiler and when the constructor function is entered through on-stack replacement (OSR). This allows for possible arbitrary reading and writing of objects during an exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.
CVE-2019-9792	The IonMonkey just-in-time (JIT) compiler can leak an internal JS_OPTIMIZED_OUT magic value to the running script during a bailout. This magic value can then be used by JavaScript to achieve memory corruption, which results in a potentially exploitable

	crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.
CVE-2019-9793	A mechanism was discovered that removes some bounds checking for string, array, or typed array accesses if Spectre mitigations have been disabled. This vulnerability could allow an attacker to create an arbitrary value in compiled JavaScript, for which the range analysis will infer a fully controlled, incorrect range in circumstances where users have explicitly disabled Spectre mitigations. *Note: Spectre mitigations are currently enabled for all users by default settings.*. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.
CVE-2019-9795	A vulnerability where type-confusion in the IonMonkey just-in-time (JIT) compiler could potentially be used by malicious JavaScript to trigger a potentially exploitable crash. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.
CVE-2019-9796	A use-after-free vulnerability can occur when the SMIL animation controller incorrectly registers with the refresh driver twice when only a single registration is expected. When a registration is later freed with the removal of the animation controller element, the refresh driver incorrectly leaves a dangling pointer to the driver's observer array. This vulnerability affects Thunderbird < 60.6, Firefox ESR < 60.6, and Firefox < 66.
CVE-2019-9797	Cross-origin images can be read in violation of the same-origin policy by exporting an image after using createImageBitmap to read the image and then rendering the resulting bitmap image within a canvas element. This vulnerability affects Firefox < 66.
CVE-2019-9800	Mozilla developers and community members reported memory safety bugs present in Firefox 66, Firefox ESR 60.6, and Thunderbird 60.6. 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 < 60.7, Firefox < 67, and Firefox ESR < 60.7.
CVE-2019-9810	Incorrect alias information in IonMonkey JIT compiler for Array.prototype.slice method may lead to missing bounds check and a buffer overflow. This vulnerability affects Firefox < 66.0.1, Firefox ESR < 60.6.1, and Thunderbird < 60.6.1.
CVE-2019-9811	As part of a winning Pwn2Own entry, a researcher demonstrated a sandbox escape by installing a malicious language pack and then opening a browser feature that used the compromised translation. This vulnerability affects Firefox ESR < 60.8, Firefox < 68, and Thunderbird < 60.8.

CVE-2019-9813	Incorrect handling of <code>__proto__</code> mutations may lead to type confusion in IonMonkey JIT code and can be leveraged for arbitrary memory read and write. This vulnerability affects Firefox < 66.0.1, Firefox ESR < 60.6.1, and Thunderbird < 60.6.1.
CVE-2019-9817	Images from a different domain can be read using a canvas object in some circumstances. This could be used to steal image data from a different site in violation of same-origin policy. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.
CVE-2019-9819	A vulnerability where a JavaScript compartment mismatch can occur while working with the fetch API, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.
CVE-2019-9820	A use-after-free vulnerability can occur in the chrome event handler when it is freed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 60.7, Firefox < 67, and Firefox ESR < 60.7.
CVE-2019-9824	tcp_emu in slirp/tcp_subr.c (aka slirp/src/tcp_subr.c) in QEMU 3.0.0 uses uninitialized data in an sprintf call, leading to Information disclosure.
CVE-2019-9893	libseccomp before 2.4.0 did not correctly generate 64-bit syscall argument comparisons using the arithmetic operators (LT, GT, LE, GE), which might be able to lead to bypassing seccomp filters and potential privilege escalations.
CVE-2019-9924	rbash in Bash before 4.4-beta2 did not prevent the shell user from modifying BASH_CMDS, thus allowing the user to execute any command with the permissions of the shell.
CVE-2019-9947	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with <code>\r\n</code> (specifically in the path component of a URL that lacks a <code>?</code> character) followed by an HTTP header or a Redis command. This is similar to the CVE-2019-9740 query string issue. This is fixed in: v2.7.17, v2.7.17rc1, v2.7.18, v2.7.18rc1; v3.5.10, v3.5.10rc1, v3.5.8, v3.5.8rc1, v3.5.8rc2, v3.5.9; v3.6.10, v3.6.10rc1, v3.6.11, v3.6.11rc1, v3.6.12, v3.6.9, v3.6.9rc1; v3.7.4, v3.7.4rc1, v3.7.4rc2, v3.7.5, v3.7.5rc1, v3.7.6, v3.7.6rc1, v3.7.7, v3.7.7rc1, v3.7.8, v3.7.8rc1, v3.7.9.
CVE-2019-9948	urllib in Python 2.x through 2.7.16 supports the <code>local_file:</code> scheme, which makes it easier for remote attackers to bypass protection mechanisms that

	blacklist file: URIs, as demonstrated by triggering a urllib.urlopen('local_file:///etc/passwd') call.
CVE-2019-9956	In ImageMagick 7.0.8-35 Q16, there is a stack-based buffer overflow in the function PopHexPixel of coders/ps.c, which allows an attacker to cause a denial of service or code execution via a crafted image file.
CVE-2019-9959	The JPXStream::init function in Poppler 0.78.0 and earlier doesn't check for negative values of stream length, leading to an Integer Overflow, thereby making it possible to allocate a large memory chunk on the heap, with a size controlled by an attacker, as demonstrated by pdftocairo.
CVE-2020-0034	In vp8_decode_frame of decodeframe.c, there is a possible out of bounds read due to improper input validation. This could lead to remote information disclosure if error correction were turned on, with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-8.0 Android-8.1 Android ID: A-62458770
CVE-2020-0093	In exif_data_save_data_entry of exif-data.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is needed for exploitation. Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10 Android ID: A-148705132
CVE-2020-0182	In exif_entry_get_value of exif-entry.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-10 Android ID: A-147140917
CVE-2020-0423	In binder_release_work of binder.c, there is a possible use-after-free due to improper locking. This could lead to local escalation of privilege in the kernel with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android kernel Android ID: A-161151868 References: N/A
CVE-2020-0452	In exif_entry_get_value of exif-entry.c, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution if a third party app used this library to process remote image data with no additional execution privileges needed. User interaction is not needed for exploitation. Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11 Android-8.0 Android ID: A-159625731
CVE-2020-0543	Incomplete cleanup from specific special register read operations in some Intel(R) Processors may allow an

	authenticated user to potentially enable information disclosure via local access.
CVE-2020-0548	Cleanup errors in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2020-0549	Cleanup errors in some data cache evictions for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2020-0556	Improper access control in subsystem for BlueZ before version 5.54 may allow an unauthenticated user to potentially enable escalation of privilege and denial of service via adjacent access
CVE-2020-0569	Out of bounds write in Intel(R) PROSet/Wireless WiFi products on Windows 10 may allow an authenticated user to potentially enable denial of service via local access.
CVE-2020-0570	Uncontrolled search path in the QT Library before 5.14.0, 5.12.7 and 5.9.10 may allow an authenticated user to potentially enable elevation of privilege via local access.
CVE-2020-10018	WebKitGTK through 2.26.4 and WPE WebKit through 2.26.4 (which are the versions right before 2.28.0) contains a memory corruption issue (use-after-free) that may lead to arbitrary code execution. This issue has been fixed in 2.28.0 with improved memory handling.
CVE-2020-10108	In Twisted Web through 19.10.0, there was an HTTP request splitting vulnerability. When presented with two content-length headers, it ignored the first header. When the second content-length value was set to zero, the request body was interpreted as a pipelined request.
CVE-2020-10109	In Twisted Web through 19.10.0, there was an HTTP request splitting vulnerability. When presented with a content-length and a chunked encoding header, the content-length took precedence and the remainder of the request body was interpreted as a pipelined request.
CVE-2020-10188	utility.c in telnetd in netkit telnet through 0.17 allows remote attackers to execute arbitrary code via short writes or urgent data, because of a buffer overflow involving the netclear and nextitem functions.
CVE-2020-10221	lib/ajaxHandlers/ajaxAddTemplate.php in rConfig through 3.94 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the fileName POST parameter.
CVE-2020-10531	An issue was discovered in International Components for Unicode (ICU) for C/C++ through 66.1. An integer overflow, leading to a heap-based buffer overflow,

	exists in the UnicodeString::doAppend() function in common/unistr.cpp.
CVE-2020-10543	Perl before 5.30.3 on 32-bit platforms allows a heap-based buffer overflow because nested regular expression quantifiers have an integer overflow.
CVE-2020-10663	The JSON gem through 2.2.0 for Ruby, as used in Ruby 2.4 through 2.4.9, 2.5 through 2.5.7, and 2.6 through 2.6.5, has an Unsafe Object Creation Vulnerability. This is quite similar to CVE-2013-0269, but does not rely on poor garbage-collection behavior within Ruby. Specifically, use of JSON parsing methods can lead to creation of a malicious object within the interpreter, with adverse effects that are application-dependent.
CVE-2020-10703	A NULL pointer dereference was found in the libvirt API responsible introduced in upstream version 3.10.0, and fixed in libvirt 6.0.0, for fetching a storage pool based on its target path. In more detail, this flaw affects storage pools created without a target path such as network-based pools like gluster and RBD. Unprivileged users with a read-only connection could abuse this flaw to crash the libvirt daemon, resulting in a potential denial of service.
CVE-2020-10711	A NULL pointer dereference flaw was found in the Linux kernel's SELinux subsystem in versions before 5.7. This flaw occurs while importing the Commercial IP Security Option (CIPSO) protocol's category bitmap into the SELinux extensible bitmap via the 'ebitmap_netlbl_import' routine. While processing the CIPSO restricted bitmap tag in the 'cipso_v4_parsetag_rbm' routine, it sets the security attribute to indicate that the category bitmap is present, even if it has not been allocated. This issue leads to a NULL pointer dereference issue while importing the same category bitmap into SELinux. This flaw allows a remote network user to crash the system kernel, resulting in a denial of service.
CVE-2020-10732	A flaw was found in the Linux kernel's implementation of Userspace core dumps. This flaw allows an attacker with a local account to crash a trivial program and exfiltrate private kernel data.
CVE-2020-10751	A flaw was found in the Linux kernels SELinux LSM hook implementation before version 5.7, where it incorrectly assumed that an skb would only contain a single netlink message. The hook would incorrectly only validate the first netlink message in the skb and allow or deny the rest of the messages within the skb with the granted permission without further processing.
CVE-2020-10754	It was found that nmcli, a command line interface to NetworkManager did not honour 802-1x.ca-path and 802-1x.phase2-ca-path settings, when creating a new

	profile. When a user connects to a network using this profile, the authentication does not happen and the connection is made insecurely.
CVE-2020-10756	An out-of-bounds read vulnerability was found in the SLiRP networking implementation of the QEMU emulator. This flaw occurs in the icmp6_send_echoReply() routine while replying to an ICMP echo request, also known as ping. This flaw allows a malicious guest to leak the contents of the host memory, resulting in possible information disclosure. This flaw affects versions of libslirp before 4.3.1.
CVE-2020-10757	A flaw was found in the Linux Kernel in versions after 4.5-rc1 in the way mremap handled DAX Huge Pages. This flaw allows a local attacker with access to a DAX enabled storage to escalate their privileges on the system.
CVE-2020-10766	A logic bug flaw was found in Linux kernel before 5.8-rc1 in the implementation of SSBD. A bug in the logic handling allows an attacker with a local account to disable SSBD protection during a context switch when additional speculative execution mitigations are in place. This issue was introduced when the per task/process conditional STIPB switching was added on top of the existing SSBD switching. The highest threat from this vulnerability is to confidentiality.
CVE-2020-10767	A flaw was found in the Linux kernel before 5.8-rc1 in the implementation of the Enhanced IBPB (Indirect Branch Prediction Barrier). The IBPB mitigation will be disabled when STIBP is not available or when the Enhanced Indirect Branch Restricted Speculation (IBRS) is available. This flaw allows a local attacker to perform a Spectre V2 style attack when this configuration is active. The highest threat from this vulnerability is to confidentiality.
CVE-2020-10768	A flaw was found in the Linux Kernel before 5.8-rc1 in the prctl() function, where it can be used to enable indirect branch speculation after it has been disabled. This call incorrectly reports it as being 'force disabled' when it is not and opens the system to Spectre v2 attacks. The highest threat from this vulnerability is to confidentiality.
CVE-2020-10772	An incomplete fix for CVE-2020-12662 was shipped for Unbound in Red Hat Enterprise Linux 7, as part of erratum RHSA-2020:2414. Vulnerable versions of Unbound could still amplify an incoming query into a large number of queries directed to a target, even with a lower amplification ratio compared to versions of Unbound that shipped before the mentioned erratum. This issue is about the incomplete fix for CVE-2020-12662, and it does not affect upstream versions of Unbound.

CVE-2020-10781	A flaw was found in the Linux Kernel before 5.8-rc6 in the ZRAM kernel module, where a user with a local account and the ability to read the /sys/class/zram-control/hot_add file can create ZRAM device nodes in the /dev/ directory. This read allocates kernel memory and is not accounted for a user that triggers the creation of that ZRAM device. With this vulnerability, continually reading the device may consume a large amount of system memory and cause the Out-of-Memory (OOM) killer to activate and terminate random userspace processes, possibly making the system inoperable.
CVE-2020-10878	Perl before 5.30.3 has an integer overflow related to mishandling of a "PL_regkind[OP(n)] == NOTHING" situation. A crafted regular expression could lead to malformed bytecode with a possibility of instruction injection.
CVE-2020-10942	In the Linux kernel before 5.5.8, get_raw_socket in drivers/vhost/net.c lacks validation of an sk_family field, which might allow attackers to trigger kernel stack corruption via crafted system calls.
CVE-2020-11008	Affected versions of Git have a vulnerability whereby Git can be tricked into sending private credentials to a host controlled by an attacker. This bug is similar to CVE-2020-5260(GHSA-qm7j-c969-7j4q). The fix for that bug still left the door open for an exploit where _some_ credential is leaked (but the attacker cannot control which one). Git uses external "credential helper" programs to store and retrieve passwords or other credentials from secure storage provided by the operating system. Specially-crafted URLs that are considered illegal as of the recently published Git versions can cause Git to send a "blank" pattern to helpers, missing hostname and protocol fields. Many helpers will interpret this as matching _any_ URL, and will return some unspecified stored password, leaking the password to an attacker's server. The vulnerability can be triggered by feeding a malicious URL to 'git clone'. However, the affected URLs look rather suspicious; the likely vector would be through systems which automatically clone URLs not visible to the user, such as Git submodules, or package systems built around Git. The root of the problem is in Git itself, which should not be feeding blank input to helpers. However, the ability to exploit the vulnerability in practice depends on which helpers are in use. Credential helpers which are known to trigger the vulnerability: - Git's "store" helper - Git's "cache" helper - the "osxkeychain" helper that ships in Git's "contrib" directory Credential helpers which are known to be safe even with vulnerable versions of Git: - Git Credential Manager for Windows Any helper not in this list should be assumed to trigger the vulnerability.

CVE-2020-11018	In FreeRDP less than or equal to 2.0.0, a possible resource exhaustion vulnerability can be performed. Malicious clients could trigger out of bound reads causing memory allocation with random size. This has been fixed in 2.1.0.
CVE-2020-11019	In FreeRDP less than or equal to 2.0.0, when running with logger set to "WLOG_TRACE", a possible crash of application could occur due to a read of an invalid array index. Data could be printed as string to local terminal. This has been fixed in 2.1.0.
CVE-2020-11022	In jQuery versions greater than or equal to 1.2 and before 3.5.0, passing HTML from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
CVE-2020-11023	In jQuery versions greater than or equal to 1.0.3 and before 3.5.0, passing HTML containing <option> elements from untrusted sources - even after sanitizing it - to one of jQuery's DOM manipulation methods (i.e. .html(), .append(), and others) may execute untrusted code. This problem is patched in jQuery 3.5.0.
CVE-2020-11038	In FreeRDP less than or equal to 2.0.0, an Integer Overflow to Buffer Overflow exists. When using /video redirection, a manipulated server can instruct the client to allocate a buffer with a smaller size than requested due to an integer overflow in size calculation. With later messages, the server can manipulate the client to write data out of bound to the previously allocated buffer. This has been patched in 2.1.0.
CVE-2020-11039	In FreeRDP less than or equal to 2.0.0, when using a manipulated server with USB redirection enabled (nearly) arbitrary memory can be read and written due to integer overflows in length checks. This has been patched in 2.1.0.
CVE-2020-11040	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound data read from memory in clear_decompress_subcode_rlex, visualized on screen as color. This has been patched in 2.1.0.
CVE-2020-11041	In FreeRDP less than or equal to 2.0.0, an outside controlled array index is used unchecked for data used as configuration for sound backend (alsa, oss, pulse, ...). The most likely outcome is a crash of the client instance followed by no or distorted sound or a session disconnect. If a user cannot upgrade to the patched version, a workaround is to disable sound for the session. This has been patched in 2.1.0.
CVE-2020-11042	In FreeRDP greater than 1.1 and before 2.0.0, there is an out-of-bounds read in update_read_icon_info.

	It allows reading a attacker-defined amount of client memory (32bit unsigned -> 4GB) to an intermediate buffer. This can be used to crash the client or store information for later retrieval. This has been patched in 2.0.0.
CVE-2020-11043	In FreeRDP less than or equal to 2.0.0, there is an out-of-bounds read in rfx_process_message_tileset. Invalid data fed to RFX decoder results in garbage on screen (as colors). This has been patched in 2.1.0.
CVE-2020-11044	In FreeRDP greater than 1.2 and before 2.0.0, a double free in update_read_cache_bitmap_v3_order crashes the client application if corrupted data from a manipulated server is parsed. This has been patched in 2.0.0.
CVE-2020-11045	In FreeRDP after 1.0 and before 2.0.0, there is an out-of-bound read in in update_read_bitmap_data that allows client memory to be read to an image buffer. The result displayed on screen as colour.
CVE-2020-11046	In FreeRDP after 1.0 and before 2.0.0, there is a stream out-of-bounds seek in update_read_synchronize that could lead to a later out-of-bounds read.
CVE-2020-11047	In FreeRDP after 1.1 and before 2.0.0, there is an out-of-bounds read in autodetect_recv_bandwidth_measure_results. A malicious server can extract up to 8 bytes of client memory with a manipulated message by providing a short input and reading the measurement result data. This has been patched in 2.0.0.
CVE-2020-11048	In FreeRDP after 1.0 and before 2.0.0, there is an out-of-bounds read. It only allows to abort a session. No data extraction is possible. This has been fixed in 2.0.0.
CVE-2020-11049	In FreeRDP after 1.1 and before 2.0.0, there is an out-of-bound read of client memory that is then passed on to the protocol parser. This has been patched in 2.0.0.
CVE-2020-11058	In FreeRDP after 1.1 and before 2.0.0, a stream out-of-bounds seek in rdp_read_font_capability_set could lead to a later out-of-bounds read. As a result, a manipulated client or server might force a disconnect due to an invalid data read. This has been fixed in 2.0.0.
CVE-2020-11080	In ngnhttp2 before version 1.41.0, the overly large HTTP/2 SETTINGS frame payload causes denial of service. The proof of concept attack involves a malicious client constructing a SETTINGS frame with a length of 14,400 bytes (2400 individual settings entries) over and over again. The attack causes the CPU to spike at 100%. ngnhttp2 v1.41.0 fixes this vulnerability. There is a workaround to this vulnerability. Implement ngnhttp2_on_frame_recv_callback callback, and if received frame is SETTINGS frame and the number

	of settings entries are large (e.g., > 32), then drop the connection.
CVE-2020-11085	In FreeRDP before 2.1.0, there is an out-of-bounds read in cliprdr_read_format_list. Clipboard format data read (by client or server) might read data out-of-bounds. This has been fixed in 2.1.0.
CVE-2020-11086	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound read in ntlm_read_ntlm_v2_client_challenge that reads up to 28 bytes out-of-bound to an internal structure. This has been fixed in 2.1.0.
CVE-2020-11087	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound read in ntlm_read_AuthenticateMessage. This has been fixed in 2.1.0.
CVE-2020-11088	In FreeRDP less than or equal to 2.0.0, there is an out-of-bound read in ntlm_read_NegotiateMessage. This has been fixed in 2.1.0.
CVE-2020-11089	In FreeRDP before 2.1.0, there is an out-of-bound read in irp functions (parallel_process_irp_create, serial_process_irp_create, drive_process_irp_write, printer_process_irp_write, rdpei_recv_pdu, serial_process_irp_write). This has been fixed in 2.1.0.
CVE-2020-11522	libfreerdp/gdi/gdi.c in FreeRDP > 1.0 through 2.0.0-rc4 has an Out-of-bounds Read.
CVE-2020-11525	libfreerdp/cache/bitmap.c in FreeRDP versions > 1.0 through 2.0.0-rc4 has an Out of bounds read.
CVE-2020-11526	libfreerdp/core/update.c in FreeRDP versions > 1.1 through 2.0.0-rc4 has an Out-of-bounds Read.
CVE-2020-11651	An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class does not properly validate method calls. This allows a remote user to access some methods without authentication. These methods can be used to retrieve user tokens from the salt master and/or run arbitrary commands on salt minions.
CVE-2020-11652	An issue was discovered in SaltStack Salt before 2019.2.4 and 3000 before 3000.2. The salt-master process ClearFuncs class allows access to some methods that improperly sanitize paths. These methods allow arbitrary directory access to authenticated users.
CVE-2020-11738	The Snap Creek Duplicator plugin before 1.3.28 for WordPress (and Duplicator Pro before 3.8.7.1) allows Directory Traversal via .. in the file parameter to duplicator_download or duplicator_init.
CVE-2020-11761	An issue was discovered in OpenEXR before 2.4.1. There is an out-of-bounds read during Huffman uncompression, as demonstrated by FastHufDecoder::refill in ImfFastHuf.cpp.

CVE-2020-11763	An issue was discovered in OpenEXR before 2.4.1. There is an std::vector out-of-bounds read and write, as demonstrated by ImfTileOffsets.cpp.
CVE-2020-11764	An issue was discovered in OpenEXR before 2.4.1. There is an out-of-bounds write in copyIntoFrameBuffer in ImfMisc.cpp.
CVE-2020-11793	A use-after-free issue exists in WebKitGTK before 2.28.1 and WPE WebKit before 2.28.1 via crafted web content that allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash).
CVE-2020-11868	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address, because transmissions are rescheduled even when a packet lacks a valid origin timestamp.
CVE-2020-11945	An issue was discovered in Squid before 5.0.2. A remote attacker can replay a snuffed Digest Authentication nonce to gain access to resources that are otherwise forbidden. This occurs because the attacker can overflow the nonce reference counter (a short integer). Remote code execution may occur if the pooled token credentials are freed (instead of replayed as valid credentials).
CVE-2020-11947	iscsi_aio_ioctl_cb in block/iscsi.c in QEMU 4.1.0 has a heap-based buffer over-read that may disclose unrelated information from process memory to an attacker.
CVE-2020-11984	Apache HTTP server 2.4.32 to 2.4.44 mod_proxy_uwsgi info disclosure and possible RCE
CVE-2020-11993	Apache HTTP Server versions 2.4.20 to 2.4.43 When trace/debug was enabled for the HTTP/2 module and on certain traffic edge patterns, logging statements were made on the wrong connection, causing concurrent use of memory pools. Configuring the LogLevel of mod_http2 above "info" will mitigate this vulnerability for unpatched servers.
CVE-2020-12100	In Dovecot before 2.3.11.3, uncontrolled recursion in submission, lmtp, and lda allows remote attackers to cause a denial of service (resource consumption) via a crafted e-mail message with deeply nested MIME parts.
CVE-2020-12243	In filter.c in slapd in OpenLDAP before 2.4.50, LDAP search filters with nested boolean expressions can result in denial of service (daemon crash).
CVE-2020-12351	Improper input validation in BlueZ may allow an unauthenticated user to potentially enable escalation of privilege via adjacent access.

CVE-2020-12352	Improper access control in BlueZ may allow an unauthenticated user to potentially enable information disclosure via adjacent access.
CVE-2020-12387	A race condition when running shutdown code for Web Worker led to a use-after-free vulnerability. This resulted in a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0.
CVE-2020-12392	The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP POST data of a request, which can be controlled by the website. If a user used the 'Copy as cURL' feature and pasted the command into a terminal, it could have resulted in the disclosure of local files. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0.
CVE-2020-12395	Mozilla developers and community members reported memory safety bugs present in Firefox 75 and Firefox ESR 68.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0.
CVE-2020-12397	By encoding Unicode whitespace characters within the From email header, an attacker can spoof the sender email address that Thunderbird displays. This vulnerability affects Thunderbird < 68.8.0.
CVE-2020-12398	If Thunderbird is configured to use STARTTLS for an IMAP server, and the server sends a PREAUTH response, then Thunderbird will continue with an unencrypted connection, causing email data to be sent without protection. This vulnerability affects Thunderbird < 68.9.0.
CVE-2020-12400	When converting coordinates from projective to affine, the modular inversion was not performed in constant time, resulting in a possible timing-based side channel attack. This vulnerability affects Firefox < 80 and Firefox for Android < 80.
CVE-2020-12401	During ECDSA signature generation, padding applied in the nonce designed to ensure constant-time scalar multiplication was removed, resulting in variable-time execution dependent on secret data. This vulnerability affects Firefox < 80 and Firefox for Android < 80.
CVE-2020-12402	During RSA key generation, bignum implementations used a variation of the Binary Extended Euclidean Algorithm which entailed significantly input-dependent flow. This allowed an attacker able to perform electromagnetic-based side channel attacks to record traces leading to the recovery of the secret primes. *Note:* An unmodified Firefox browser does not generate RSA keys in normal operation and is not

	affected, but products built on top of it might. This vulnerability affects Firefox < 78.
CVE-2020-12403	A flaw was found in the way CHACHA20-POLY1305 was implemented in NSS in versions before 3.55. When using multi-part Chacha20, it could cause out-of-bounds reads. This issue was fixed by explicitly disabling multi-part ChaCha20 (which was not functioning correctly) and strictly enforcing tag length. The highest threat from this vulnerability is to confidentiality and system availability.
CVE-2020-12405	When browsing a malicious page, a race condition in our SharedWorkerService could occur and lead to a potentially exploitable crash. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9.
CVE-2020-12406	Mozilla Developer Iain Ireland discovered a missing type check during unboxed objects removal, resulting in a crash. We presume that with enough effort that it could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9.
CVE-2020-12410	Mozilla developers reported memory safety bugs present in Firefox 76 and Firefox ESR 68.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.9.0, Firefox < 77, and Firefox ESR < 68.9.
CVE-2020-12417	Due to confusion about ValueTags on JavaScript Objects, an object may pass through the type barrier, resulting in memory corruption and a potentially exploitable crash. *Note: this issue only affects Firefox on ARM64 platforms.* This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.
CVE-2020-12418	Manipulating individual parts of a URL object could have caused an out-of-bounds read, leaking process memory to malicious JavaScript. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.
CVE-2020-12419	When processing callbacks that occurred during window flushing in the parent process, the associated window may die; causing a use-after-free condition. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.
CVE-2020-12420	When trying to connect to a STUN server, a race condition could have caused a use-after-free of a pointer, leading to memory corruption and a potentially

	exploitable crash. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.
CVE-2020-12421	When performing add-on updates, certificate chains terminating in non-built-in-roots were rejected (even if they were legitimately added by an administrator.) This could have caused add-ons to become out-of-date silently without notification to the user. This vulnerability affects Firefox ESR < 68.10, Firefox < 78, and Thunderbird < 68.10.0.
CVE-2020-12655	An issue was discovered in xfs_agf_verify in fs/xfs/libxfs/xfs_alloc.c in the Linux kernel through 5.6.10. Attackers may trigger a sync of excessive duration via an XFS v5 image with crafted metadata, aka CID-d0c7feaf8767.
CVE-2020-12656	** DISPUTED ** gss_mech_free in net/sunrpc/auth_gss/gss_mech_switch.c in the rpcsec_gss_krb5 implementation in the Linux kernel through 5.6.10 lacks certain domain_release calls, leading to a memory leak. Note: This was disputed with the assertion that the issue does not grant any access not already available. It is a problem that on unloading a specific kernel module some memory is leaked, but loading kernel modules is a privileged operation. A user could also write a kernel module to consume any amount of memory they like and load that replicating the effect of this bug.
CVE-2020-12657	An issue was discovered in the Linux kernel before 5.6.5. There is a use-after-free in block/bfq-iosched.c related to bfq_idle_slice_timer_body.
CVE-2020-12662	Unbound before 1.10.1 has Insufficient Control of Network Message Volume, aka an "NXNSAttack" issue. This is triggered by random subdomains in the NSDNAME in NS records.
CVE-2020-12663	Unbound before 1.10.1 has an infinite loop via malformed DNS answers received from upstream servers.
CVE-2020-12673	In Dovecot before 2.3.11.3, sending a specially formatted NTLM request will crash the auth service because of an out-of-bounds read.
CVE-2020-12674	In Dovecot before 2.3.11.3, sending a specially formatted RPA request will crash the auth service because a length of zero is mishandled.
CVE-2020-12723	regcomp.c in Perl before 5.30.3 allows a buffer overflow via a crafted regular expression because of recursive S_study_chunk calls.
CVE-2020-12762	json-c through 0.14 has an integer overflow and out-of-bounds write via a large JSON file, as demonstrated by printbuf_memappend.

CVE-2020-12767	exif_entry_get_value in exif-entry.c in libexif 0.6.21 has a divide-by-zero error.
CVE-2020-12768	** DISPUTED ** An issue was discovered in the Linux kernel before 5.6. svm_cpu_uninit in arch/x86/kvm/svm.c has a memory leak, aka CID-d80b64ff297e. NOTE: third parties dispute this issue because it's a one-time leak at the boot, the size is negligible, and it can't be triggered at will.
CVE-2020-12770	An issue was discovered in the Linux kernel through 5.6.11. sg_write lacks an sg_remove_request call in a certain failure case, aka CID-83c6f2390040.
CVE-2020-12771	An issue was discovered in the Linux kernel through 5.6.11. btree_gc_coalesce in drivers/md/bcache/btree.c has a deadlock if a coalescing operation fails.
CVE-2020-12825	libcroco through 0.6.13 has excessive recursion in cr_parser_parse_any_core in cr-parser.c, leading to stack consumption.
CVE-2020-12826	A signal access-control issue was discovered in the Linux kernel before 5.6.5, aka CID-7395ea4e65c2. Because exec_id in include/linux/sched.h is only 32 bits, an integer overflow can interfere with a do_notify_parent protection mechanism. A child process can send an arbitrary signal to a parent process in a different security domain. Exploitation limitations include the amount of elapsed time before an integer overflow occurs, and the lack of scenarios where signals to a parent process present a substantial operational threat.
CVE-2020-12888	The VFIO PCI driver in the Linux kernel through 5.6.13 mishandles attempts to access disabled memory space.
CVE-2020-13112	An issue was discovered in libexif before 0.6.22. Several buffer over-reads in EXIF MakerNote handling could lead to information disclosure and crashes. This is different from CVE-2020-0093.
CVE-2020-13113	An issue was discovered in libexif before 0.6.22. Use of uninitialized memory in EXIF Makernote handling could lead to crashes and potential use-after-free conditions.
CVE-2020-13114	An issue was discovered in libexif before 0.6.22. An unrestricted size in handling Canon EXIF MakerNote data could lead to consumption of large amounts of compute time for decoding EXIF data.
CVE-2020-13143	gadget_dev_desc_UDC_store in drivers/usb/gadget/configfs.c in the Linux kernel 3.16 through 5.6.13 relies on kstrdup without considering the possibility of an internal '\0' value, which allows attackers to trigger an out-of-bounds read, aka CID-15753588bcd4.
CVE-2020-13396	An issue was discovered in FreeRDP before 2.1.1. An out-of-bounds (OOB) read vulnerability has been

	detected in ntlm_read_ChallengeMessage in winpr/libwinpr/sspi/NTLM/ntlm_message.c.
CVE-2020-13397	An issue was discovered in FreeRDP before 2.1.1. An out-of-bounds (OOB) read vulnerability has been detected in security_fips_decrypt in libfreerdp/core/security.c due to an uninitialized value.
CVE-2020-13401	An issue was discovered in Docker Engine before 19.03.11. An attacker in a container, with the CAP_NET_RAW capability, can craft IPv6 router advertisements, and consequently spoof external IPv6 hosts, obtain sensitive information, or cause a denial of service.
CVE-2020-13692	PostgreSQL JDBC Driver (aka PgJDBC) before 42.2.13 allows XXE.
CVE-2020-13757	Python-RSA before 4.1 ignores leading '\0' bytes during decryption of ciphertext. This could conceivably have a security-relevant impact, e.g., by helping an attacker to infer that an application uses Python-RSA, or if the length of accepted ciphertext affects application behavior (such as by causing excessive memory allocation).
CVE-2020-13765	rom_copy() in hw/core/loader.c in QEMU 4.0 and 4.1.0 does not validate the relationship between two addresses, which allows attackers to trigger an invalid memory copy operation.
CVE-2020-13817	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows remote attackers to cause a denial of service (daemon exit or system time change) by predicting transmit timestamps for use in spoofed packets. The victim must be relying on unauthenticated IPv4 time sources. There must be an off-path attacker who can query time from the victim's ntpd instance.
CVE-2020-13867	Open-iSCSI targetcli-fb through 2.1.52 has weak permissions for /etc/target (and for the backup directory and backup files).
CVE-2020-13935	The payload length in a WebSocket frame was not correctly validated in Apache Tomcat 10.0.0-M1 to 10.0.0-M6, 9.0.0.M1 to 9.0.36, 8.5.0 to 8.5.56 and 7.0.27 to 7.0.104. Invalid payload lengths could trigger an infinite loop. Multiple requests with invalid payload lengths could lead to a denial of service.
CVE-2020-13936	An attacker that is able to modify Velocity templates may execute arbitrary Java code or run arbitrary system commands with the same privileges as the account running the Servlet container. This applies to applications that allow untrusted users to upload/modify velocity templates running Apache Velocity Engine versions up to 2.2.

CVE-2020-13938	Apache HTTP Server versions 2.4.0 to 2.4.46 Unprivileged local users can stop httpd on Windows
CVE-2020-13946	In Apache Cassandra, all versions prior to 2.1.22, 2.2.18, 3.0.22, 3.11.8 and 4.0-beta2, it is possible for a local attacker without access to the Apache Cassandra process or configuration files to manipulate the RMI registry to perform a man-in-the-middle attack and capture user names and passwords used to access the JMX interface. The attacker can then use these credentials to access the JMX interface and perform unauthorised operations. Users should also be aware of CVE-2019-2684, a JRE vulnerability that enables this issue to be exploited remotely.
CVE-2020-13950	Apache HTTP Server versions 2.4.41 to 2.4.46 mod_proxy_http can be made to crash (NULL pointer dereference) with specially crafted requests using both Content-Length and Transfer-Encoding headers, leading to a Denial of Service
CVE-2020-14019	Open-iSCSI rtslib-fb through 2.1.72 has weak permissions for /etc/target/saveconfig.json because shutil.copyfile (instead of shutil.copy) is used, and thus permissions are not preserved.
CVE-2020-14040	The x/text package before 0.3.3 for Go has a vulnerability in encoding/unicode that could lead to the UTF-16 decoder entering an infinite loop, causing the program to crash or run out of memory. An attacker could provide a single byte to a UTF16 decoder instantiated with UseBOM or ExpectBOM to trigger an infinite loop if the String function on the Decoder is called, or the Decoder is passed to golang.org/x/text/transform.String.
CVE-2020-14175	Affected versions of Atlassian Confluence Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in user macro parameters. The affected versions are before version 7.4.2, and from version 7.5.0 before 7.5.2.
CVE-2020-14312	A flaw was found in the default configuration of dnsmasq, as shipped with Fedora versions prior to 31 and in all versions Red Hat Enterprise Linux, where it listens on any interface and accepts queries from addresses outside of its local subnet. In particular, the option `local-service` is not enabled. Running dnsmasq in this manner may inadvertently make it an open resolver accessible from any address on the internet. This flaw allows an attacker to conduct a Distributed Denial of Service (DDoS) against other systems.
CVE-2020-14314	A memory out-of-bounds read flaw was found in the Linux kernel before 5.9-rc2 with the ext3/ext4 file system, in the way it accesses a directory with broken

	<p>indexing. This flaw allows a local user to crash the system if the directory exists. The highest threat from this vulnerability is to system availability.</p>
CVE-2020-14318	A flaw was found in the way samba handled file and directory permissions. An authenticated user could use this flaw to gain access to certain file and directory information which otherwise would be unavailable to the attacker.
CVE-2020-14323	A null pointer dereference flaw was found in samba's Winbind service in versions before 4.11.15, before 4.12.9 and before 4.13.1. A local user could use this flaw to crash the winbind service causing denial of service.
CVE-2020-14331	A flaw was found in the Linux kernel's implementation of the invert video code on VGA consoles when a local attacker attempts to resize the console, calling an ioctl VT_RESIZE, which causes an out-of-bounds write to occur. This flaw allows a local user with access to the VGA console to crash the system, potentially escalating their privileges on the system. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14344	An integer overflow leading to a heap-buffer overflow was found in The X Input Method (XIM) client was implemented in libX11 before version 1.6.10. As per upstream this is security relevant when setuid programs call XIM client functions while running with elevated privileges. No such programs are shipped with Red Hat Enterprise Linux.
CVE-2020-14345	A flaw was found in X.Org Server before xorg-x11-server 1.20.9. An Out-Of-Bounds access in XkbSetNames function may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14346	A flaw was found in xorg-x11-server before 1.20.9. An integer underflow in the X input extension protocol decoding in the X server may lead to arbitrary access of memory contents. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14347	A flaw was found in the way xserver memory was not properly initialized. This could leak parts of server memory to the X client. In cases where Xorg server runs with elevated privileges, this could result in possible ASLR bypass. Xorg-server before version 1.20.9 is vulnerable.
CVE-2020-14351	A flaw was found in the Linux kernel. A use-after-free memory flaw was found in the perf subsystem allowing a local attacker with permission to monitor

	perf events to corrupt memory and possibly escalate privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14352	A flaw was found in librepo in versions before 1.12.1. A directory traversal vulnerability was found where it failed to sanitize paths in remote repository metadata. An attacker controlling a remote repository may be able to copy files outside of the destination directory on the targeted system via path traversal. This flaw could potentially result in system compromise via the overwriting of critical system files. The highest threat from this flaw is to users that make use of untrusted third-party repositories.
CVE-2020-14355	Multiple buffer overflow vulnerabilities were found in the QUIC image decoding process of the SPICE remote display system, before spice-0.14.2-1. Both the SPICE client (spice-gtk) and server are affected by these flaws. These flaws allow a malicious client or server to send specially crafted messages that, when processed by the QUIC image compression algorithm, result in a process crash or potential code execution.
CVE-2020-14360	A flaw was found in the X.Org Server before version 1.20.10. An out-of-bounds access in the XkbSetMap function may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14361	A flaw was found in X.Org Server before xorg-x11-server 1.20.9. An Integer underflow leading to heap-buffer overflow may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14362	A flaw was found in X.Org Server before xorg-x11-server 1.20.9. An Integer underflow leading to heap-buffer overflow may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-14363	An integer overflow vulnerability leading to a double-free was found in libX11. This flaw allows a local privileged attacker to cause an application compiled with libX11 to crash, or in some cases, result in arbitrary code execution. The highest threat from this flaw is to confidentiality, integrity as well as system availability.
CVE-2020-14364	An out-of-bounds read/write access flaw was found in the USB emulator of the QEMU in versions before 5.2.0. This issue occurs while processing USB packets from a guest when USBDevice 'setup_len' exceeds its 'data_buf[4096]' in the do_token_in, do_token_out

	routines. This flaw allows a guest user to crash the QEMU process, resulting in a denial of service, or the potential execution of arbitrary code with the privileges of the QEMU process on the host.
CVE-2020-14367	A flaw was found in chrony versions before 3.5.1 when creating the PID file under the /var/run/chrony folder. The file is created during chronyd startup while still running as the root user, and when it's opened for writing, chronyd does not check for an existing symbolic link with the same file name. This flaw allows an attacker with privileged access to create a symlink with the default PID file name pointing to any destination file in the system, resulting in data loss and a denial of service due to the path traversal.
CVE-2020-14372	A flaw was found in grub2 in versions prior to 2.06, where it incorrectly enables the usage of the ACPI command when Secure Boot is enabled. This flaw allows an attacker with privileged access to craft a Secondary System Description Table (SSDT) containing code to overwrite the Linux kernel lockdown variable content directly into memory. The table is further loaded and executed by the kernel, defeating its Secure Boot lockdown and allowing the attacker to load unsigned code. The highest threat from this vulnerability is to data confidentiality and integrity, as well as system availability.
CVE-2020-14385	A flaw was found in the Linux kernel before 5.9-rc4. A failure of the file system metadata validator in XFS can cause an inode with a valid, user-creatable extended attribute to be flagged as corrupt. This can lead to the filesystem being shutdown, or otherwise rendered inaccessible until it is remounted, leading to a denial of service. The highest threat from this vulnerability is to system availability.
CVE-2020-14386	A flaw was found in the Linux kernel before 5.9-rc4. Memory corruption can be exploited to gain root privileges from unprivileged processes. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2020-14390	A flaw was found in the Linux kernel in versions before 5.9-rc6. When changing screen size, an out-of-bounds memory write can occur leading to memory corruption or a denial of service. Due to the nature of the flaw, privilege escalation cannot be fully ruled out.
CVE-2020-14422	Lib/ipaddress.py in Python through 3.8.3 improperly computes hash values in the IPv4Interface and IPv6Interface classes, which might allow a remote attacker to cause a denial of service if an application is affected by the performance of a dictionary containing IPv4Interface or IPv6Interface objects, and this attacker can cause many dictionary entries to be created. This

	is fixed in: v3.5.10, v3.5.10rc1; v3.6.12; v3.7.9; v3.8.4, v3.8.4rc1, v3.8.5, v3.8.6, v3.8.6rc1; v3.9.0, v3.9.0b4, v3.9.0b5, v3.9.0rc1, v3.9.0rc2.
CVE-2020-14556	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:A:N).
CVE-2020-14562	Vulnerability in the Java SE product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 11.0.7 and 14.0.1. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14573	Vulnerability in the Java SE product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 11.0.7 and 14.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start

	<p>applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).</p>
CVE-2020-14577	<p>Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).</p>
CVE-2020-14578	<p>Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).</p>
CVE-2020-14579	<p>Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261 and 8u251; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful</p>

	<p>attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).</p>
CVE-2020-14581	<p>Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).</p>
CVE-2020-14583	<p>Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability)</p>

	impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2020-14593	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: 2D). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.4 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:N/I:H/A:N).
CVE-2020-14621	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JAXP). Supported versions that are affected are Java SE: 7u261, 8u251, 11.0.7 and 14.0.1; Java SE Embedded: 8u251. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14664	Vulnerability in the Java SE product of Oracle Java SE (component: JavaFX). The supported version that is affected is Java SE: 8u251. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of

	<p>this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).</p>
CVE-2020-1472	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.
CVE-2020-14734	Vulnerability in the Oracle Text component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Oracle Net to compromise Oracle Text. Successful attacks of this vulnerability can result in takeover of Oracle Text. CVSS 3.1 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-14735	Vulnerability in the Scheduler component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Scheduler executes to compromise Scheduler. While the vulnerability is in Scheduler, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Scheduler. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H).
CVE-2020-14736	Vulnerability in the Database Vault component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows high privileged attacker having Create Public Synonym privilege with network access via Oracle Net to compromise Database Vault. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Database Vault accessible data as well as unauthorized read access to a subset of Database Vault accessible data. CVSS 3.1 Base Score 3.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).

	Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-14740	Vulnerability in the SQL Developer Install component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1 and 18c. Easily exploitable vulnerability allows low privileged attacker having Client Computer User Account privilege with logon to the infrastructure where SQL Developer Install executes to compromise SQL Developer Install. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of SQL Developer Install accessible data. CVSS 3.1 Base Score 2.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:N/A:N).
CVE-2020-14741	Vulnerability in the Database Filesystem component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2 and 12.2.0.1. Easily exploitable vulnerability allows high privileged attacker having Resource, Create Table, Create View, Create Procedure, Dbfs_role privilege with network access via Oracle Net to compromise Database Filesystem. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Database Filesystem. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-14742	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having SYSDBA level account privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Core RDBMS accessible data. CVSS 3.1 Base Score 2.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14779	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed

	Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-14781	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JNDI). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-14782	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14792	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java

	SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:A:N).
CVE-2020-14796	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).
CVE-2020-14797	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying

	data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2020-14798	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u271, 8u261, 11.0.8 and 15; Java SE Embedded: 8u261. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2020-14803	Vulnerability in the Java SE product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 11.0.8 and 15. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-14901	Vulnerability in the RDBMS Security component of Oracle Database Server. The supported version that is affected is 19c. Easily exploitable vulnerability allows high privileged attacker having Analyze Any privilege with network access via Oracle Net to compromise RDBMS Security. Successful attacks of this vulnerability can result in unauthorized access

	to critical data or complete access to all RDBMS Security accessible data. CVSS 3.1 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).
CVE-2020-15157	In containerd (an industry-standard container runtime) before version 1.2.14 there is a credential leaking vulnerability. If a container image manifest in the OCI Image format or Docker Image V2 Schema 2 format includes a URL for the location of a specific image layer (otherwise known as a “foreign layer”), the default containerd resolver will follow that URL to attempt to download it. In v1.2.x but not 1.3.0 or later, the default containerd resolver will provide its authentication credentials if the server where the URL is located presents an HTTP 401 status code along with registry-specific HTTP headers. If an attacker publishes a public image with a manifest that directs one of the layers to be fetched from a web server they control and they trick a user or system into pulling the image, they can obtain the credentials used for pulling that image. In some cases, this may be the user's username and password for the registry. In other cases, this may be the credentials attached to the cloud virtual instance which can grant access to other cloud resources in the account. The default containerd resolver is used by the cri-containerd plugin (which can be used by Kubernetes), the ctr development tool, and other client programs that have explicitly linked against it. This vulnerability has been fixed in containerd 1.2.14. containerd 1.3 and later are not affected. If you are using containerd 1.3 or later, you are not affected. If you are using cri-containerd in the 1.2 series or prior, you should ensure you only pull images from trusted sources. Other container runtimes built on top of containerd but not using the default resolver (such as Docker) are not affected.
CVE-2020-15257	containerd is an industry-standard container runtime and is available as a daemon for Linux and Windows. In containerd before versions 1.3.9 and 1.4.3, the containerd-shim API is improperly exposed to host network containers. Access controls for the shim's API socket verified that the connecting process had an effective UID of 0, but did not otherwise restrict access to the abstract Unix domain socket. This would allow malicious containers running in the same network namespace as the shim, with an effective UID of 0 but otherwise reduced privileges, to cause new processes to be run with elevated privileges. This vulnerability has been fixed in containerd 1.3.9 and 1.4.3. Users should update to these versions as soon as they are released. It should be noted that containers started with an old version of containerd-shim should be stopped

	<p>and restarted, as running containers will continue to be vulnerable even after an upgrade. If you are not providing the ability for untrusted users to start containers in the same network namespace as the shim (typically the "host" network namespace, for example with docker run --net=host or hostNetwork: true in a Kubernetes pod) and run with an effective UID of 0, you are not vulnerable to this issue. If you are running containers with a vulnerable configuration, you can deny access to all abstract sockets with AppArmor by adding a line similar to deny unix addr=@**, to your policy. It is best practice to run containers with a reduced set of privileges, with a non-zero UID, and with isolated namespaces. The containerd maintainers strongly advise against sharing namespaces with the host. Reducing the set of isolation mechanisms used for a container necessarily increases that container's privilege, regardless of what container runtime is used for running that container.</p>
CVE-2020-15389	jp2/opj_decompress.c in OpenJPEG through 2.3.1 has a use-after-free that can be triggered if there is a mix of valid and invalid files in a directory operated on by the decompressor. Triggering a double-free may also be possible. This is related to calling opj_image_destroy twice.
CVE-2020-15393	In the Linux kernel 4.4 through 5.7.6, usbtest_disconnect in drivers/usb/misc/usbtest.c has a memory leak, aka CID-28ebeb8db770.
CVE-2020-15586	Go before 1.13.13 and 1.14.x before 1.14.5 has a data race in some net/http servers, as demonstrated by the httputil.ReverseProxy Handler, because it reads a request body and writes a response at the same time.
CVE-2020-15652	By observing the stack trace for JavaScript errors in web workers, it was possible to leak the result of a cross-origin redirect. This applied only to content that can be parsed as script. This vulnerability affects Firefox < 79, Firefox ESR < 68.11, Firefox ESR < 78.1, Thunderbird < 68.11, and Thunderbird < 78.1.
CVE-2020-15659	Mozilla developers and community members reported memory safety bugs present in Firefox 78 and Firefox ESR 78.0. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 79, Firefox ESR < 68.11, Firefox ESR < 78.1, Thunderbird < 68.11, and Thunderbird < 78.1.
CVE-2020-15664	By holding a reference to the eval() function from an about:blank window, a malicious webpage could have gained access to the InstallTrigger object which would allow them to prompt the user to install an extension. Combined with user confusion, this could result in an

	unintended or malicious extension being installed. This vulnerability affects Firefox < 80, Thunderbird < 78.2, Thunderbird < 68.12, Firefox ESR < 68.12, Firefox ESR < 78.2, and Firefox for Android < 80.
CVE-2020-15669	When aborting an operation, such as a fetch, an abort signal may be deleted while alerting the objects to be notified. This results in a use-after-free and we presume that with enough effort it could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 68.12 and Thunderbird < 68.12.
CVE-2020-15673	Mozilla developers reported memory safety bugs present in Firefox 80 and Firefox ESR 78.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3.
CVE-2020-15676	Firefox sometimes ran the onload handler for SVG elements that the DOM sanitizer decided to remove, resulting in JavaScript being executed after pasting attacker-controlled data into a contenteditable element. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3.
CVE-2020-15677	By exploiting an Open Redirect vulnerability on a website, an attacker could have spoofed the site displayed in the download file dialog to show the original site (the one suffering from the open redirect) rather than the site the file was actually downloaded from. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3.
CVE-2020-15678	When recursing through graphical layers while scrolling, an iterator may have become invalid, resulting in a potential use-after-free. This occurs because the function APZCTreeManager::ComputeClippedCompositionBounds did not follow iterator invalidation rules. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3.
CVE-2020-15683	Mozilla developers and community members reported memory safety bugs present in Firefox 81 and Firefox ESR 78.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 78.4, Firefox < 82, and Thunderbird < 78.4.
CVE-2020-15685	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

CVE-2020-15810	An issue was discovered in Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Smuggling attacks may succeed against HTTP and HTTPS traffic. This leads to cache poisoning. This allows any client, including browser scripts, to bypass local security and poison the proxy cache and any downstream caches with content from an arbitrary source. When configured for relaxed header parsing (the default), Squid relays headers containing whitespace characters to upstream servers. When this occurs as a prefix to a Content-Length header, the frame length specified will be ignored by Squid (allowing for a conflicting length to be used from another Content-Length header) but relayed upstream.
CVE-2020-15811	An issue was discovered in Squid before 4.13 and 5.x before 5.0.4. Due to incorrect data validation, HTTP Request Splitting attacks may succeed against HTTP and HTTPS traffic. This leads to cache poisoning. This allows any client, including browser scripts, to bypass local security and poison the browser cache and any downstream caches with content from an arbitrary source. Squid uses a string search instead of parsing the Transfer-Encoding header to find chunked encoding. This allows an attacker to hide a second request inside Transfer-Encoding: it is interpreted by Squid as chunked and split out into a second request delivered upstream. Squid will then deliver two distinct responses to the client, corrupting any downstream caches.
CVE-2020-15862	Net-SNMP through 5.7.3 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides the ability to run arbitrary commands as root.
CVE-2020-15959	Insufficient policy enforcement in networking in Google Chrome prior to 85.0.4183.102 allowed an attacker who convinced the user to enable logging to obtain potentially sensitive information from process memory via social engineering.
CVE-2020-15960	Heap buffer overflow in storage in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2020-15961	Insufficient policy validation in extensions in Google Chrome prior to 85.0.4183.121 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2020-15962	Insufficient policy validation in serial in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.

CVE-2020-15963	Insufficient policy enforcement in extensions in Google Chrome prior to 85.0.4183.121 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2020-15964	Insufficient data validation in media in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15965	Type confusion in V8 in Google Chrome prior to 85.0.4183.121 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2020-15966	Insufficient policy enforcement in extensions in Google Chrome prior to 85.0.4183.121 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information via a crafted Chrome Extension.
CVE-2020-15967	Use after free in payments in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-15968	Use after free in Blink in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15969	Use after free in WebRTC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15970	Use after free in NFC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-15971	Use after free in printing in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-15972	Use after free in audio in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15973	Insufficient policy enforcement in extensions in Google Chrome prior to 86.0.4240.75 allowed an attacker who convinced a user to install a malicious extension to bypass same origin policy via a crafted Chrome Extension.
CVE-2020-15974	Integer overflow in Blink in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to bypass site isolation via a crafted HTML page.

CVE-2020-15975	Integer overflow in SwiftShader in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15976	Use after free in WebXR in Google Chrome on Android prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15977	Insufficient data validation in dialogs in Google Chrome on OS X prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from disk via a crafted HTML page.
CVE-2020-15978	Insufficient data validation in navigation in Google Chrome on Android prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.
CVE-2020-15979	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15980	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 86.0.4240.75 allowed a local attacker to bypass navigation restrictions via crafted Intents.
CVE-2020-15981	Out of bounds read in audio in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-15982	Inappropriate implementation in cache in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-15983	Insufficient data validation in webUI in Google Chrome on ChromeOS prior to 86.0.4240.75 allowed a local attacker to bypass content security policy via a crafted HTML page.
CVE-2020-15984	Insufficient policy enforcement in Omnibox in Google Chrome on iOS prior to 86.0.4240.75 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted URL.
CVE-2020-15985	Inappropriate implementation in Blink in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-15986	Integer overflow in media in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2020-15987	Use after free in WebRTC in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to potentially exploit heap corruption via a crafted WebRTC stream.
CVE-2020-15988	Insufficient policy enforcement in downloads in Google Chrome on Windows prior to 86.0.4240.75 allowed a remote attacker who convinced the user to open files to execute arbitrary code via a crafted HTML page.
CVE-2020-15989	Uninitialized data in PDFium in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.
CVE-2020-15990	Use after free in autofill in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-15991	Use after free in password manager in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-15992	Insufficient policy enforcement in networking in Google Chrome prior to 86.0.4240.75 allowed a remote attacker who had compromised the renderer process to bypass same origin policy via a crafted HTML page.
CVE-2020-15995	Out of bounds write in V8 in Google Chrome prior to 86.0.4240.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-15999	Heap buffer overflow in Freetype in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16000	Inappropriate implementation in Blink in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16001	Use after free in media in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16002	Use after free in PDFium in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2020-16003	Use after free in printing in Google Chrome prior to 86.0.4240.111 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16004	Use after free in user interface in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2020-16005	Insufficient policy enforcement in ANGLE in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16006	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16007	Insufficient data validation in installer in Google Chrome prior to 86.0.4240.183 allowed a local attacker to potentially elevate privilege via a crafted filesystem.
CVE-2020-16008	Stack buffer overflow in WebRTC in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit stack corruption via a crafted WebRTC packet.
CVE-2020-16009	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.183 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16012	Side-channel information leakage in graphics in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-16013	Inappropriate implementation in V8 in Google Chrome prior to 86.0.4240.198 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16014	Use after free in PPAPI in Google Chrome prior to 87.0.4280.66 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-16015	Insufficient data validation in WASM in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16016	Inappropriate implementation in base in Google Chrome prior to 86.0.4240.193 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-16017	Use after free in site isolation in Google Chrome prior to 86.0.4240.198 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-16018	Use after free in payments in Google Chrome prior to 87.0.4280.66 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-16019	Inappropriate implementation in filesystem in Google Chrome on ChromeOS prior to 87.0.4280.66 allowed

	a remote attacker who had compromised the browser process to bypass noexec restrictions via a malicious file.
CVE-2020-16020	Inappropriate implementation in cryptohome in Google Chrome on ChromeOS prior to 87.0.4280.66 allowed a remote attacker who had compromised the browser process to bypass discretionary access control via a malicious file.
CVE-2020-16021	Race in image burner in Google Chrome on ChromeOS prior to 87.0.4280.66 allowed a remote attacker who had compromised the browser process to perform OS-level privilege escalation via a malicious file.
CVE-2020-16022	Insufficient policy enforcement in networking in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to potentially bypass firewall controls via a crafted HTML page.
CVE-2020-16023	Use after free in WebCodecs in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16024	Heap buffer overflow in UI in Google Chrome prior to 87.0.4280.66 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-16025	Heap buffer overflow in clipboard in Google Chrome prior to 87.0.4280.66 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-16026	Use after free in WebRTC in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16027	Insufficient policy enforcement in developer tools in Google Chrome prior to 87.0.4280.66 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from the user's disk via a crafted Chrome Extension.
CVE-2020-16028	Heap buffer overflow in WebRTC in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16029	Inappropriate implementation in PDFium in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to bypass navigation restrictions via a crafted PDF file.
CVE-2020-16030	Insufficient data validation in Blink in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2020-16031	Insufficient data validation in UI in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to spoof the

	contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-16032	Insufficient data validation in sharing in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-16033	Inappropriate implementation in WebUSB in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-16034	Inappropriate implementation in WebRTC in Google Chrome prior to 87.0.4280.66 allowed a local attacker to bypass policy restrictions via a crafted HTML page.
CVE-2020-16035	Insufficient data validation in cros-disks in Google Chrome on ChromeOS prior to 87.0.4280.66 allowed a remote attacker who had compromised the browser process to bypass noexec restrictions via a malicious file.
CVE-2020-16036	Inappropriate implementation in cookies in Google Chrome prior to 87.0.4280.66 allowed a remote attacker to bypass cookie restrictions via a crafted HTML page.
CVE-2020-16037	Use after free in clipboard in Google Chrome prior to 87.0.4280.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16038	Use after free in media in Google Chrome on OS X prior to 87.0.4280.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16039	Use after free in extensions in Google Chrome prior to 87.0.4280.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16040	Insufficient data validation in V8 in Google Chrome prior to 87.0.4280.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-16041	Out of bounds read in networking in Google Chrome prior to 87.0.4280.88 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-16042	Uninitialized Use in V8 in Google Chrome prior to 87.0.4280.88 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-16043	Insufficient data validation in networking in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to bypass discretionary access control via malicious network traffic.

CVE-2020-16044	Use after free in WebRTC in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted SCTP packet.
CVE-2020-16092	In QEMU through 5.0.0, an assertion failure can occur in the network packet processing. This issue affects the e1000e and vmxnet3 network devices. A malicious guest user/process could use this flaw to abort the QEMU process on the host, resulting in a denial of service condition in net_tx_pkt_add_raw_fragment in hw/net/net_tx_pkt.c.
CVE-2020-16119	Use-after-free vulnerability in the Linux kernel exploitable by a local attacker due to reuse of a DCCP socket with an attached dccps_hc_tx_ccid object as a listener after being released. Fixed in Ubuntu Linux kernel 5.4.0-51.56, 5.3.0-68.63, 4.15.0-121.123, 4.4.0-193.224, 3.13.0-182.191 and 3.2.0-149.196.
CVE-2020-16166	The Linux kernel through 5.7.11 allows remote attackers to make observations that help to obtain sensitive information about the internal state of the network RNG, aka CID-f227e3ec3b5c. This is related to drivers/char/random.c and kernel/time/timer.c.
CVE-2020-16845	Go before 1.13.15 and 14.x before 1.14.7 can have an infinite read loop in ReadUvarint and ReadVarint in encoding/binary via invalid inputs.
CVE-2020-1711	An out-of-bounds heap buffer access flaw was found in the way the iSCSI Block driver in QEMU versions 2.12.0 before 4.2.1 handled a response coming from an iSCSI server while checking the status of a Logical Address Block (LBA) in an iscsi_co_block_status() routine. A remote user could use this flaw to crash the QEMU process, resulting in a denial of service or potential execution of arbitrary code with privileges of the QEMU process on the host.
CVE-2020-1712	A heap use-after-free vulnerability was found in systemd before version v245-rc1, where asynchronous Polkit queries are performed while handling dbus messages. A local unprivileged attacker can abuse this flaw to crash systemd services or potentially execute code and elevate their privileges, by sending specially crafted dbus messages.
CVE-2020-1721	A flaw was found in the Key Recovery Authority (KRA) Agent Service in pki-core 10.10.5 where it did not properly sanitize the recovery ID during a key recovery request, enabling a reflected cross-site scripting (XSS) vulnerability. An attacker could trick an authenticated victim into executing specially crafted Javascript code.
CVE-2020-1722	A flaw was found in all ipa versions 4.x.x through 4.8.0. When sending a very long password (>= 1,000,000 characters) to the server, the password hashing process could exhaust memory and CPU leading

	<p>to a denial of service and the website becoming unresponsive. The highest threat from this vulnerability is to system availability.</p>
CVE-2020-1749	A flaw was found in the Linux kernel's implementation of some networking protocols in IPsec, such as VXLAN and GENEVE tunnels over IPv6. When an encrypted tunnel is created between two hosts, the kernel isn't correctly routing tunneled data over the encrypted link; rather sending the data unencrypted. This would allow anyone in between the two endpoints to read the traffic unencrypted. The main threat from this vulnerability is to data confidentiality.
CVE-2020-17507	An issue was discovered in Qt through 5.12.9, and 5.13.x through 5.15.x before 5.15.1. <code>read_xbm_body</code> in <code>gui/image/qxbmhandler.cpp</code> has a buffer over-read.
CVE-2020-17516	Apache Cassandra versions 2.1.0 to 2.1.22, 2.2.0 to 2.2.19, 3.0.0 to 3.0.23, and 3.11.0 to 3.11.9, when using 'dc' or 'rack' internode_encryption setting, allows both encrypted and unencrypted internode connections. A misconfigured node or a malicious user can use the unencrypted connection despite not being in the same rack or dc, and bypass mutual TLS requirement.
CVE-2020-1927	In Apache HTTP Server 2.4.0 to 2.4.41, redirects configured with mod_rewrite that were intended to be self-referential might be fooled by encoded newlines and redirect instead to an unexpected URL within the request URL.
CVE-2020-1934	In Apache HTTP Server 2.4.0 to 2.4.41, mod_proxy_ftp may use uninitialized memory when proxying to a malicious FTP server.
CVE-2020-1938	When using the Apache JServ Protocol (AJP), care must be taken when trusting incoming connections to Apache Tomcat. Tomcat treats AJP connections as having higher trust than, for example, a similar HTTP connection. If such connections are available to an attacker, they can be exploited in ways that may be surprising. In Apache Tomcat 9.0.0.M1 to 9.0.0.30, 8.5.0 to 8.5.50 and 7.0.0 to 7.0.99, Tomcat shipped with an AJP Connector enabled by default that listened on all configured IP addresses. It was expected (and recommended in the security guide) that this Connector would be disabled if not required. This vulnerability report identified a mechanism that allowed:

	mitigation is only required if an AJP port is accessible to untrusted users. Users wishing to take a defence-in-depth approach and block the vector that permits returning arbitrary files and execution as JSP may upgrade to Apache Tomcat 9.0.31, 8.5.51 or 7.0.100 or later. A number of changes were made to the default AJP Connector configuration in 9.0.31 to harden the default configuration. It is likely that users upgrading to 9.0.31, 8.5.51 or 7.0.100 or later will need to make small changes to their configurations.
CVE-2020-1946	In Apache SpamAssassin before 3.4.5, malicious rule configuration (.cf) files can be configured to run system commands without any output or errors. With this, exploits can be injected in a number of scenarios. In addition to upgrading to SA version 3.4.5, users should only use update channels or 3rd party .cf files from trusted places.
CVE-2020-1971	The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMES contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified. OpenSSL's s_server, s_client and verify tools have support for the "-crl_download" option which implements automatic CRL downloading and this attack has been demonstrated to work against those tools. Note that an unrelated bug means that affected versions of OpenSSL cannot parse or construct correct encodings of EDIPARTYNAME. However it is possible to construct a malformed EDIPARTYNAME that OpenSSL's parser will accept and hence trigger this attack. All OpenSSL 1.1.1 and 1.0.2 versions

	are affected by this issue. Other OpenSSL releases are out of support and have not been checked. Fixed in OpenSSL 1.1.1i (Affected 1.1.1-1.1.1h). Fixed in OpenSSL 1.0.2x (Affected 1.0.2-1.0.2w).
CVE-2020-1983	A use after free vulnerability in ip_reass() in ip_input.c of libslirp 4.2.0 and prior releases allows crafted packets to cause a denial of service.
CVE-2020-2099	Jenkins 2.213 and earlier, LTS 2.204.1 and earlier improperly reuses encryption key parameters in the Inbound TCP Agent Protocol/3, allowing unauthorized attackers with knowledge of agent names to obtain the connection secrets for those agents, which can be used to connect to Jenkins, impersonating those agents.
CVE-2020-2100	Jenkins 2.218 and earlier, LTS 2.204.1 and earlier was vulnerable to a UDP amplification reflection denial of service attack on port 33848.
CVE-2020-2101	Jenkins 2.218 and earlier, LTS 2.204.1 and earlier did not use a constant-time comparison function for validating connection secrets, which could potentially allow an attacker to use a timing attack to obtain this secret.
CVE-2020-2102	Jenkins 2.218 and earlier, LTS 2.204.1 and earlier used a non-constant time comparison function when validating an HMAC.
CVE-2020-2103	Jenkins 2.218 and earlier, LTS 2.204.1 and earlier exposed session identifiers on a user's detail object in the whoAmI diagnostic page.
CVE-2020-2104	Jenkins 2.218 and earlier, LTS 2.204.1 and earlier allowed users with Overall/Read access to view a JVM memory usage chart.
CVE-2020-2105	REST API endpoints in Jenkins 2.218 and earlier, LTS 2.204.1 and earlier were vulnerable to clickjacking attacks.
CVE-2020-2160	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier uses different representations of request URL paths, which allows attackers to craft URLs that allow bypassing CSRF protection of any target URL.
CVE-2020-2161	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier does not properly escape node labels that are shown in the form validation for label expressions on job configuration pages, resulting in a stored XSS vulnerability exploitable by users able to define node labels.
CVE-2020-2162	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier does not set Content-Security-Policy headers for files uploaded as file parameters to a build, resulting in a stored XSS vulnerability.
CVE-2020-2163	Jenkins 2.227 and earlier, LTS 2.204.5 and earlier improperly processes HTML content of list view

	column headers, resulting in a stored XSS vulnerability exploitable by users able to control column headers.
CVE-2020-2220	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape the agent name in the build time trend page, resulting in a stored cross-site scripting vulnerability.
CVE-2020-2221	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape the upstream job's display name shown as part of a build cause, resulting in a stored cross-site scripting vulnerability.
CVE-2020-2222	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape the job name in the 'Keep this build forever' badge tooltip, resulting in a stored cross-site scripting vulnerability.
CVE-2020-2223	Jenkins 2.244 and earlier, LTS 2.235.1 and earlier does not escape correctly the 'href' attribute of links to downstream jobs displayed in the build console page, resulting in a stored cross-site scripting vulnerability.
CVE-2020-2229	Jenkins 2.251 and earlier, LTS 2.235.3 and earlier does not escape the tooltip content of help icons, resulting in a stored cross-site scripting (XSS) vulnerability.
CVE-2020-2230	Jenkins 2.251 and earlier, LTS 2.235.3 and earlier does not escape the project naming strategy description, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by users with Overall/Manage permission.
CVE-2020-2231	Jenkins 2.251 and earlier, LTS 2.235.3 and earlier does not escape the remote address of the host starting a build via 'Trigger builds remotely', resulting in a stored cross-site scripting (XSS) vulnerability exploitable by users with Job/Configure permission or knowledge of the Authentication Token.
CVE-2020-24370	ldebug.c in Lua 5.4.0 allows a negation overflow and segmentation fault in getlocal and setlocal, as demonstrated by getlocal(3,2^31).
CVE-2020-24490	Improper buffer restrictions in BlueZ may allow an unauthenticated user to potentially enable denial of service via adjacent access. This affects all Linux kernel versions that support BlueZ.
CVE-2020-24553	Go before 1.14.8 and 1.15.x before 1.15.1 allows XSS because text/html is the default for CGI/FCGI handlers that lack a Content-Type header.
CVE-2020-24586	The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that received fragments be cleared from memory after (re)connecting to a network. Under the right circumstances, when another device sends fragmented frames encrypted using WEP, CCMP, or GCMP, this can be abused to

	inject arbitrary network packets and/or exfiltrate user data.
CVE-2020-24587	The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that all fragments of a frame are encrypted under the same key. An adversary can abuse this to decrypt selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP encryption key is periodically renewed.
CVE-2020-24588	The 802.11 standard that underpins Wi-Fi Protected Access (WPA, WPA2, and WPA3) and Wired Equivalent Privacy (WEP) doesn't require that the A-MSDU flag in the plaintext QoS header field is authenticated. Against devices that support receiving non-SSP A-MSDU frames (which is mandatory as part of 802.11n), an adversary can abuse this to inject arbitrary network packets.
CVE-2020-24606	Squid before 4.13 and 5.x before 5.0.4 allows a trusted peer to perform Denial of Service by consuming all available CPU cycles during handling of a crafted Cache Digest response message. This only occurs when cache_peer is used with the cache digests feature. The problem exists because peerDigestHandleReply() livelocking in peer_digest.cc mishandles EOF.
CVE-2020-24977	GNOME project libxml2 v2.9.10 has a global buffer over-read vulnerability in xmlEncodeEntitiesInternal at libxml2/entities.c. The issue has been fixed in commit 50f06b3e.
CVE-2020-25097	An issue was discovered in Squid through 4.13 and 5.x through 5.0.4. Due to improper input validation, it allows a trusted client to perform HTTP Request Smuggling and access services otherwise forbidden by the security controls. This occurs for certain uri_whitespace configuration settings.
CVE-2020-2510	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via OracleNet to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Core RDBMS. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).
CVE-2020-2511	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily

	exploitable vulnerability allows low privileged attacker having Create Session privilege with network access via OracleNet to compromise Core RDBMS. While the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Core RDBMS. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).
CVE-2020-2512	Vulnerability in the Database Gateway for ODBC component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows unauthenticated attacker with network access via OracleNet to compromise Database Gateway for ODBC. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Database Gateway for ODBC. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2515	Vulnerability in the Database Gateway for ODBC component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via OracleNet to compromise Database Gateway for ODBC. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Database Gateway for ODBC accessible data as well as unauthorized read access to a subset of Database Gateway for ODBC accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Database Gateway for ODBC. CVSS 3.0 Base Score 5.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L).
CVE-2020-2516	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Materialized View, Create Table privilege with network access via OracleNet to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Core RDBMS accessible data. CVSS 3.0 Base Score 2.4 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:N/I:L/A:N).

CVE-2020-2517	Vulnerability in the Database Gateway for ODBC component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c, and 19c. Difficult to exploit vulnerability allows high privileged attacker having Create Procedure, Create Database Link privilege with network access via OracleNet to compromise Database Gateway for ODBC. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Database Gateway for ODBC accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Database Gateway for ODBC. CVSS 3.0 Base Score 3.3 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:L).
CVE-2020-2518	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via multiple protocols to compromise Java VM. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-25211	In the Linux kernel through 5.8.7, local attackers able to inject conntrack netlink configuration could overflow a local buffer, causing crashes or triggering use of incorrect protocol numbers in ctnetlink_parse_tuple_filter in net/netfilter/nf_conntrack_netlink.c, aka CID-1cc5ef91d2ff.
CVE-2020-25212	A TOCTOU mismatch in the NFS client code in the Linux kernel before 5.8.3 could be used by local attackers to corrupt memory or possibly have unspecified other impact because a size check is in fs/nfs/nfs4proc.c instead of fs/nfs/nfs4xdr.c, aka CID-b4487b935452.
CVE-2020-2527	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Create Index, Create Table privilege with network access via OracleNet to compromise Core RDBMS. While the vulnerability is in Core RDBMS, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Core RDBMS accessible data. CVSS 3.0 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:L/I:N/A:N).

CVE-2020-25284	The rbd block device driver in drivers/block/rbd.c in the Linux kernel through 5.8.9 used incomplete permission checking for access to rbd devices, which could be leveraged by local attackers to map or unmap rbd block devices, aka CID-f44d04e696fe.
CVE-2020-25285	A race condition between hugetlb sysctl handlers in mm/hugetlb.c in the Linux kernel before 5.8.8 could be used by local attackers to corrupt memory, cause a NULL pointer dereference, or possibly have unspecified other impact, aka CID-17743798d812.
CVE-2020-25613	An issue was discovered in Ruby through 2.5.8, 2.6.x through 2.6.6, and 2.7.x through 2.7.1. WEBrick, a simple HTTP server bundled with Ruby, had not checked the transfer-encoding header value rigorously. An attacker may potentially exploit this issue to bypass a reverse proxy (which also has a poor header check), which may lead to an HTTP Request Smuggling attack.
CVE-2020-25632	A flaw was found in grub2 in versions prior to 2.06. The rmmod implementation allows the unloading of a module used as a dependency without checking if any other dependent module is still loaded leading to a use-after-free scenario. This could allow arbitrary code to be executed or a bypass of Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25637	A double free memory issue was found to occur in the libvirt API, in versions before 6.8.0, responsible for requesting information about network interfaces of a running QEMU domain. This flaw affects the polkit access control driver. Specifically, clients connecting to the read-write socket with limited ACL permissions could use this flaw to crash the libvirt daemon, resulting in a denial of service, or potentially escalate their privileges on the system. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25639	A NULL pointer dereference flaw was found in the Linux kernel's GPU Nouveau driver functionality in versions prior to 5.12-rc1 in the way the user calls ioctl DRM_IOCTL_NOUVEAU_CHANNEL_ALLOC. This flaw allows a local user to crash the system.
CVE-2020-25641	A flaw was found in the Linux kernel's implementation of biovecs in versions before 5.9-rc7. A zero-length biovec request issued by the block subsystem could cause the kernel to enter an infinite loop, causing a denial of service. This flaw allows a local attacker with basic privileges to issue requests to a block device, resulting in a denial of service. The highest threat from this vulnerability is to system availability.

CVE-2020-25643	A flaw was found in the HDLC_PPP module of the Linux kernel in versions before 5.9-rc7. Memory corruption and a read overflow is caused by improper input validation in the ppp_cp_parse_cr function which can cause the system to crash or cause a denial of service. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25645	A flaw was found in the Linux kernel in versions before 5.9-rc7. Traffic between two Geneve endpoints may be unencrypted when IPsec is configured to encrypt traffic for the specific UDP port used by the GENEVE tunnel allowing anyone between the two endpoints to read the traffic unencrypted. The main threat from this vulnerability is to data confidentiality.
CVE-2020-25647	A flaw was found in grub2 in versions prior to 2.06. During USB device initialization, descriptors are read with very little bounds checking and assumes the USB device is providing sane values. If properly exploited, an attacker could trigger memory corruption leading to arbitrary code execution allowing a bypass of the Secure Boot mechanism. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25648	A flaw was found in the way NSS handled CCS (ChangeCipherSpec) messages in TLS 1.3. This flaw allows a remote attacker to send multiple CCS messages, causing a denial of service for servers compiled with the NSS library. The highest threat from this vulnerability is to system availability. This flaw affects NSS versions before 3.58.
CVE-2020-25654	An ACL bypass flaw was found in pacemaker. An attacker having a local account on the cluster and in the haclient group could use IPC communication with various daemons directly to perform certain tasks that they would be prevented by ACLs from doing if they went through the configuration.
CVE-2020-25656	A flaw was found in the Linux kernel. A use-after-free was found in the way the console subsystem was using ioctls KDGKBSENT and KDSKBSENT. A local user could use this flaw to get read memory access out of bounds. The highest threat from this vulnerability is to data confidentiality.
CVE-2020-25668	A flaw was found in Linux Kernel because access to the global variable fg_console is not properly synchronized leading to a use after free in con_font_op.
CVE-2020-25669	A vulnerability was found in the Linux Kernel where the function sunkbd_reinit having been scheduled by sunkbd_interrupt before sunkbd being freed. Though the dangling pointer is set to

	NULL in sunkbd_disconnect, there is still an alias in sunkbd_reinit causing Use After Free.
CVE-2020-25670	A vulnerability was found in Linux Kernel where refcount leak in llcp_sock_bind() causing use-after-free which might lead to privilege escalations.
CVE-2020-25671	A vulnerability was found in Linux Kernel, where a refcount leak in llcp_sock_connect() causing use-after-free which might lead to privilege escalations.
CVE-2020-25672	A memory leak vulnerability was found in Linux kernel in llcp_sock_connect
CVE-2020-25673	A vulnerability was found in Linux kernel where non-blocking socket in llcp_sock_connect() leads to leak and eventually hanging-up the system.
CVE-2020-2568	Vulnerability in the Oracle Applications DBA component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Oracle Applications DBA executes to compromise Oracle Applications DBA. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications DBA accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Applications DBA. CVSS 3.0 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L).
CVE-2020-25684	A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in the forward.c:reply_query() if the reply destination address/port is used by the pending forwarded queries. However, it does not use the address/port to retrieve the exact forwarded query, substantially reducing the number of attempts an attacker on the network would have to perform to forge a reply and get it accepted by dnsmasq. This issue contrasts with RFC5452, which specifies a query's attributes that all must be used to match a reply. This flaw allows an attacker to perform a DNS Cache Poisoning attack. If chained with CVE-2020-25685 or CVE-2020-25686, the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.
CVE-2020-25685	A flaw was found in dnsmasq before version 2.83. When getting a reply from a forwarded query, dnsmasq checks in forward.c:reply_query(), which is the forwarded query that matches the reply, by only using a weak hash of the query name. Due to the weak hash (CRC32 when dnsmasq is compiled without

	DNSSEC, SHA-1 when it is) this flaw allows an off-path attacker to find several different domains all having the same hash, substantially reducing the number of attempts they would have to perform to forge a reply and get it accepted by dnsmasq. This is in contrast with RFC5452, which specifies that the query name is one of the attributes of a query that must be used to match a reply. This flaw could be abused to perform a DNS Cache Poisoning attack. If chained with CVE-2020-25684 the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.
CVE-2020-25686	A flaw was found in dnsmasq before version 2.83. When receiving a query, dnsmasq does not check for an existing pending request for the same name and forwards a new request. By default, a maximum of 150 pending queries can be sent to upstream servers, so there can be at most 150 queries for the same name. This flaw allows an off-path attacker on the network to substantially reduce the number of attempts that it would have to perform to forge a reply and have it accepted by dnsmasq. This issue is mentioned in the "Birthday Attacks" section of RFC5452. If chained with CVE-2020-25684, the attack complexity of a successful attack is reduced. The highest threat from this vulnerability is to data integrity.
CVE-2020-2569	Vulnerability in the Oracle Applications DBA component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Oracle Applications DBA executes to compromise Oracle Applications DBA. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Applications DBA accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Applications DBA. CVSS 3.0 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L).
CVE-2020-25692	A NULL pointer dereference was found in OpenLDAP server and was fixed in openldap 2.4.55, during a request for renaming RDNs. An unauthenticated attacker could remotely crash the slapd process by sending a specially crafted request, causing a Denial of Service.
CVE-2020-25694	A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. If a client application that creates additional database connections only reuses the basic

	connection parameters while dropping security-relevant parameters, an opportunity for a man-in-the-middle attack, or the ability to observe clear-text transmissions, could exist. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25695	A flaw was found in PostgreSQL versions before 13.1, before 12.5, before 11.10, before 10.15, before 9.6.20 and before 9.5.24. An attacker having permission to create non-temporary objects in at least one schema can execute arbitrary SQL functions under the identity of a superuser. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25704	A flaw memory leak in the Linux kernel performance monitoring subsystem was found in the way if using PERF_EVENT_IOC_SET_FILTER. A local user could use this flaw to starve the resources causing denial of service.
CVE-2020-25709	A flaw was found in OpenLDAP. This flaw allows an attacker who can send a malicious packet to be processed by OpenLDAP's slapd server, to trigger an assertion failure. The highest threat from this vulnerability is to system availability.
CVE-2020-25710	A flaw was found in OpenLDAP in versions before 2.4.56. This flaw allows an attacker who sends a malicious packet processed by OpenLDAP to force a failed assertion in csnNormalize23(). The highest threat from this vulnerability is to system availability.
CVE-2020-25712	A flaw was found in xorg-x11-server before 1.20.10. A heap-buffer overflow in XkbSetDeviceInfo may lead to a privilege escalation vulnerability. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-25715	A flaw was found in pki-core 10.9.0. A specially crafted POST request can be used to reflect a DOM-based cross-site scripting (XSS) attack to inject code into the search query form which can get automatically executed. The highest threat from this vulnerability is to data integrity.
CVE-2020-25717	A flaw was found in the way Samba maps domain users to local users. An authenticated attacker could use this flaw to cause possible privilege escalation.
CVE-2020-25723	A reachable assertion issue was found in the USB EHCI emulation code of QEMU. It could occur while processing USB requests due to missing handling of DMA memory map failure. A malicious privileged user within the guest may abuse this flaw to send bogus USB requests and crash the QEMU process on the host, resulting in a denial of service.

CVE-2020-2574	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.46 and prior, 5.7.28 and prior and 8.0.18 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2583	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2585	Vulnerability in the Java SE product of Oracle Java SE (component: JavaFX). The supported version that is affected is Java SE: 8u231. 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 creation, deletion or modification access to critical data or all Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).
CVE-2020-2590	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security).

	<p>Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).</p>
CVE-2020-2593	<p>Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:A:N).</p>
CVE-2020-2601	<p>Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Kerberos to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded</p>

	accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).
CVE-2020-2604	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS v3.0 Base Score 8.1 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H).
CVE-2020-26116	http.client in Python 3.x before 3.5.10, 3.6.x before 3.6.12, 3.7.x before 3.7.9, and 3.8.x before 3.8.5 allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of HTTPConnection.request.
CVE-2020-26137	urllib3 before 1.25.9 allows CRLF injection if the attacker controls the HTTP request method, as demonstrated by inserting CR and LF control characters in the first argument of putrequest(). NOTE: this is similar to CVE-2020-26116.
CVE-2020-26139	An issue was discovered in the kernel in NetBSD 7.1. An Access Point (AP) forwards EAPOL frames to other clients even though the sender has not yet successfully authenticated to the AP. This might be abused in projected Wi-Fi networks to launch denial-of-service attacks against connected clients and makes it easier to exploit other vulnerabilities in connected clients.
CVE-2020-26141	An issue was discovered in the ALFA Windows 10 driver 6.1316.1209 for AWUS036H. The Wi-Fi

	implementation does not verify the Message Integrity Check (authenticity) of fragmented TKIP frames. An adversary can abuse this to inject and possibly decrypt packets in WPA or WPA2 networks that support the TKIP data-confidentiality protocol.
CVE-2020-26145	An issue was discovered on Samsung Galaxy S3 i9305 4.4.4 devices. The WEP, WPA, WPA2, and WPA3 implementations accept second (or subsequent) broadcast fragments even when sent in plaintext and process them as full unfragmented frames. An adversary can abuse this to inject arbitrary network packets independent of the network configuration.
CVE-2020-26147	An issue was discovered in the Linux kernel 5.8.9. The WEP, WPA, WPA2, and WPA3 implementations reassemble fragments even though some of them were sent in plaintext. This vulnerability can be abused to inject packets and/or exfiltrate selected fragments when another device sends fragmented frames and the WEP, CCMP, or GCMP data-confidentiality protocol is used.
CVE-2020-26217	XStream before version 1.4.14 is vulnerable to Remote Code Execution. The vulnerability may allow a remote attacker to run arbitrary shell commands only by manipulating the processed input stream. Only users who rely on blocklists are affected. Anyone using XStream's Security Framework allowlist is not affected. The linked advisory provides code workarounds for users who cannot upgrade. The issue is fixed in version 1.4.14.
CVE-2020-2654	Vulnerability in the Java SE product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u241, 8u231, 11.0.5 and 13.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-26541	The Linux kernel through 5.8.13 does not properly enforce the Secure Boot Forbidden Signature Database (aka dbx) protection mechanism. This affects certs/blacklist.c and certs/system_keyring.c.
CVE-2020-2655	Vulnerability in the Java SE product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 11.0.5 and 13.0.1. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Java

	SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data as well as unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-26558	Bluetooth LE and BR/EDR secure pairing in Bluetooth Core Specification 2.1 through 5.2 may permit a nearby man-in-the-middle attacker to identify the Passkey used during pairing (in the Passkey authentication procedure) by reflection of the public key and the authentication evidence of the initiating device, potentially permitting this attacker to complete authenticated pairing with the responding device using the correct Passkey for the pairing session. The attack methodology determines the Passkey value one bit at a time.
CVE-2020-2659	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u241 and 8u231; Java SE Embedded: 8u231. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-26950	In certain circumstances, the MCallGetProperty opcode can be emitted with unmet assumptions resulting in an exploitable use-after-free condition. This vulnerability affects Firefox < 82.0.3, Firefox ESR < 78.4.1, and Thunderbird < 78.4.2.
CVE-2020-26951	A parsing and event loading mismatch in Firefox's SVG code could have allowed load events to fire, even after

	sanitization. An attacker already capable of exploiting an XSS vulnerability in privileged internal pages could have used this attack to bypass our built-in sanitizer. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26953	It was possible to cause the browser to enter fullscreen mode without displaying the security UI; thus making it possible to attempt a phishing attack or otherwise confuse the user. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26956	In some cases, removing HTML elements during sanitization would keep existing SVG event handlers and therefore lead to XSS. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26958	Firefox did not block execution of scripts with incorrect MIME types when the response was intercepted and cached through a ServiceWorker. This could lead to a cross-site script inclusion vulnerability, or a Content Security Policy bypass. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26959	During browser shutdown, reference decrementing could have occurred on a previously freed object, resulting in a use-after-free, memory corruption, and a potentially exploitable crash. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26960	If the Compact() method was called on an nsTArray, the array could have been reallocated without updating other pointers, leading to a potential use-after-free and exploitable crash. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26961	When DNS over HTTPS is in use, it intentionally filters RFC1918 and related IP ranges from the responses as these do not make sense coming from a DoH resolver. However when an IPv4 address was mapped through IPv6, these addresses were erroneously let through, leading to a potential DNS Rebinding attack. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26965	Some websites have a feature "Show Password" where clicking a button will change a password field into a textbook field, revealing the typed password. If, when using a software keyboard that remembers user input, a user typed their password and used that feature, the type of the password field was changed, resulting in a keyboard layout change and the possibility for the software keyboard to remember the typed password. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.

CVE-2020-26968	Mozilla developers reported memory safety bugs present in Firefox 82 and Firefox ESR 78.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 83, Firefox ESR < 78.5, and Thunderbird < 78.5.
CVE-2020-26971	Certain blit values provided by the user were not properly constrained leading to a heap buffer overflow on some video drivers. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.
CVE-2020-26973	Certain input to the CSS Sanitizer confused it, resulting in incorrect components being removed. This could have been used as a sanitizer bypass. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.
CVE-2020-26974	When flex-basis was used on a table wrapper, a StyleGenericFlexBasis object could have been incorrectly cast to the wrong type. This resulted in a heap user-after-free, memory corruption, and a potentially exploitable crash. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.
CVE-2020-26976	When a HTTPS pages was embedded in a HTTP page, and there was a service worker registered for the former, the service worker could have intercepted the request for the secure page despite the iframe not being a secure context due to the (insecure) framing. This vulnerability affects Firefox < 84.
CVE-2020-26978	Using techniques that built on the slipstream research, a malicious webpage could have exposed both an internal network's hosts as well as services running on the user's local machine. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.
CVE-2020-27171	An issue was discovered in the Linux kernel before 5.11.8. kernel/bpf/verifier.c has an off-by-one error (with a resultant integer underflow) affecting out-of-bounds speculation on pointer arithmetic, leading to side-channel attacks that defeat Spectre mitigations and obtain sensitive information from kernel memory, aka CID-10d2bb2e6b1d.
CVE-2020-2731	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows low privileged attacker having Local Logon privilege with logon to the infrastructure where Core RDBMS executes to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker. Successful attacks of

	this vulnerability can result in unauthorized update, insert or delete access to some of Core RDBMS accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Core RDBMS. CVSS 3.0 Base Score 3.9 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:R/S:U/C:N/I:L/A:L).
CVE-2020-2732	A flaw was discovered in the way that the KVM hypervisor handled instruction emulation for an L2 guest when nested virtualisation is enabled. Under some circumstances, an L2 guest may trick the L0 guest into accessing sensitive L1 resources that should be inaccessible to the L2 guest.
CVE-2020-2734	Vulnerability in the RDBMS/Optimizer component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having Execute on DBMS_SQLTUNE privilege with network access via Oracle Net to compromise RDBMS/Optimizer. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of RDBMS/Optimizer accessible data. CVSS 3.0 Base Score 2.4 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:R/S:U/C:L/I:N/A:N).
CVE-2020-2735	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session privilege with network access via Oracle Net to compromise Java VM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java VM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.0 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H).
CVE-2020-2737	Vulnerability in the Core RDBMS component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows high privileged attacker having Create Session, Execute Catalog Role privilege with network access via Oracle Net to compromise Core RDBMS. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Core RDBMS. CVSS 3.0 Base Score 6.4 (Confidentiality, Integrity and Availability impacts).

	CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:R/S:U/C:H/I:H/A:H).
CVE-2020-2752	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.47 and prior, 5.7.27 and prior and 8.0.17 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-27534	util/binfmt_misc/check.go in Builder in Docker Engine before 19.03.9 calls os.OpenFile with a potentially unsafe qemu-check temporary pathname, constructed with an empty first argument in an ioutil.TempDir call.
CVE-2020-2754	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions that are affected are Java SE: 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2755	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Scripting). Supported versions that are affected are Java SE: 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start

	applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2756	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-2757	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Serialization). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-27618	The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid multi-byte input sequences in IBM1364, IBM1371, IBM1388, IBM1390, and IBM1399 encodings, fails to advance the input state, which could lead to an infinite loop in applications, resulting in a denial of service, a different vulnerability from CVE-2016-10228.

CVE-2020-27619	In Python 3 through 3.9.0, the Lib/test/multibytecodec_support.py CJK codec tests call eval() on content retrieved via HTTP.
CVE-2020-2767	Vulnerability in the Java SE product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 11.0.6 and 14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data as well as unauthorized read access to a subset of Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).
CVE-2020-27673	An issue was discovered in the Linux kernel through 5.9.1, as used with Xen through 4.14.x. Guest OS users can cause a denial of service (host OS hang) via a high rate of events to dom0, aka CID-e99502f76271.
CVE-2020-27675	An issue was discovered in the Linux kernel through 5.9.1, as used with Xen through 4.14.x. drivers/xen/events/events_base.c allows event-channel removal during the event-handling loop (a race condition). This can cause a use-after-free or NULL pointer dereference, as demonstrated by a dom0 crash via events for an in-reconfiguration paravirtualized device, aka CID-073d0552ead5.
CVE-2020-2773	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Security). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS

	3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-27749	A flaw was found in grub2 in versions prior to 2.06. Variable names present are expanded in the supplied command line into their corresponding variable contents, using a 1kB stack buffer for temporary storage, without sufficient bounds checking. If the function is called with a command line that references a variable with a sufficiently large payload, it is possible to overflow the stack buffer, corrupt the stack frame and control execution which could also circumvent Secure Boot protections. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-27777	A flaw was found in the way RTAS handled memory accesses in userspace to kernel communication. On a locked down (usually due to Secure Boot) guest system running on top of PowerVM or KVM hypervisors (pseries platform) a root like local user could use this flaw to further increase their privileges to that of a running kernel.
CVE-2020-27779	A flaw was found in grub2 in versions prior to 2.06. The cutmem command does not honor secure boot locking allowing an privileged attacker to remove address ranges from memory creating an opportunity to circumvent SecureBoot protections after proper triage about grub's memory layout. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-2778	Vulnerability in the Java SE product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 11.0.6 and 14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-27783	A XSS vulnerability was discovered in python-lxml's clean module. The module's parser didn't properly imitate browsers, which caused different behaviors between the sanitizer and the user's page. A remote

	attacker could exploit this flaw to run arbitrary HTML/JS code.
CVE-2020-2780	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: DML). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2781	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-27814	A heap-buffer overflow was found in the way openjpeg2 handled certain PNG format files. An attacker could use this flaw to cause an application crash or in some cases execute arbitrary code with the permission of the user running such an application.
CVE-2020-27815	A flaw was found in the JFS filesystem code in the Linux Kernel which allows a local attacker with the ability to set extended attributes to panic the system, causing memory corruption or escalating privileges. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2020-27820	A vulnerability was found in Linux kernel, where a use-after-frees in nouveau's postclose() handler could happen if removing device (that is not common to remove video card physically without power-off, but same happens if "unbind" the driver).
CVE-2020-27821	A flaw was found in the memory management API of QEMU during the initialization of a memory region

	cache. This issue could lead to an out-of-bounds write access to the MSI-X table while performing MMIO operations. A guest user may abuse this flaw to crash the QEMU process on the host, resulting in a denial of service. This flaw affects QEMU versions prior to 5.2.0.
CVE-2020-27823	A flaw was found in OpenJPEG's encoder. This flaw allows an attacker to pass specially crafted x,y offset input to OpenJPEG to use during encoding. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2020-27824	A flaw was found in OpenJPEG's encoder in the opj_dwt_calc_explicit_stepsizes() function. This flaw allows an attacker who can supply crafted input to decomposition levels to cause a buffer overflow. The highest threat from this vulnerability is to system availability.
CVE-2020-27825	A use-after-free flaw was found in kernel/trace/ring_buffer.c in Linux kernel (before 5.10-rc1). There was a race problem in trace_open and resize of cpu buffer running parallelly on different cpus, may cause a denial of service problem (DOS). This flaw could even allow a local attacker with special user privilege to a kernel information leak threat.
CVE-2020-27842	There's a flaw in openjpeg's t2 encoder in versions prior to 2.4.0. An attacker who is able to provide crafted input to be processed by openjpeg could cause a null pointer dereference. The highest impact of this flaw is to application availability.
CVE-2020-27843	A flaw was found in OpenJPEG in versions prior to 2.4.0. This flaw allows an attacker to provide specially crafted input to the conversion or encoding functionality, causing an out-of-bounds read. The highest threat from this vulnerability is system availability.
CVE-2020-27844	A flaw was found in openjpeg's src/lib/openjp2/t2.c in versions prior to 2.4.0. This flaw allows an attacker to provide crafted input to openjpeg during conversion and encoding, causing an out-of-bounds write. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2020-27845	There's a flaw in src/lib/openjp2/pi.c of openjpeg in versions prior to 2.4.0. If an attacker is able to provide untrusted input to openjpeg's conversion/encoding functionality, they could cause an out-of-bounds read. The highest impact of this flaw is to application availability.
CVE-2020-2800	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Lightweight HTTP Server). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability

	<p>allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 4.8 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N).</p>
CVE-2020-2803	<p>Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R:S:C/C:H/I:H/A:H).</p>
CVE-2020-2805	<p>Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments,</p>

	typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2020-2812	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Stored Procedure). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2020-2816	Vulnerability in the Java SE product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 11.0.6 and 14. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTPS to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE accessible data. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).
CVE-2020-2830	Vulnerability in the Java SE, Java SE Embedded product of Oracle Java SE (component: Concurrency). Supported versions that are affected are Java SE: 7u251, 8u241, 11.0.6 and 14; Java SE Embedded: 8u241. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed

	Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2020-28362	Go before 1.14.12 and 1.15.x before 1.15.4 allows Denial of Service.
CVE-2020-28366	Go before 1.14.12 and 1.15.x before 1.15.5 allows Code Injection.
CVE-2020-28367	Code injection in the go command with cgo before Go 1.14.12 and Go 1.15.5 allows arbitrary code execution at build time via malicious gcc flags specified via a #cgo directive.
CVE-2020-28374	In drivers/target/target_core_xcopy.c in the Linux kernel before 5.10.7, insufficient identifier checking in the LIO SCSI target code can be used by remote attackers to read or write files via directory traversal in an XCOPY request, aka CID-2896c93811e3. For example, an attack can occur over a network if the attacker has access to one iSCSI LUN. The attacker gains control over file access because I/O operations are proxied via an attacker-selected backstore.
CVE-2020-28916	hw/net/e1000e_core.c in QEMU 5.0.0 has an infinite loop via an RX descriptor with a NULL buffer address.
CVE-2020-28935	NLnet Labs Unbound, up to and including version 1.12.0, and NLnet Labs NSD, up to and including version 4.3.3, contain a local vulnerability that would allow for a local symlink attack. When writing the PID file, Unbound and NSD create the file if it is not there, or open an existing file for writing. In case the file was already present, they would follow symlinks if the file happened to be a symlink instead of a regular file. An additional chown of the file would then take place after it was written, making the user Unbound/NSD is supposed to run as the new owner of the file. If an attacker has local access to the user Unbound/NSD runs as, she could create a symlink in place of the PID file pointing to a file that she would like to erase. If then Unbound/NSD is killed and the PID file is not cleared, upon restarting with root privileges, Unbound/NSD will rewrite any file pointed at by the symlink. This is a local vulnerability that could create a Denial of Service of the system Unbound/NSD is running on. It requires an attacker having access to the limited permission user Unbound/NSD runs as and point through the symlink to a critical file on the system.
CVE-2020-28941	An issue was discovered in drivers/accessibility/speakup/spk_ttyio.c in the Linux kernel through 5.9.9. Local attackers on systems with the speakup driver could cause a local denial of service attack, aka CID-d41227544427. This occurs because of an invalid free when the line discipline is used more than once.

CVE-2020-28948	Archive_Tar through 1.4.10 allows an unserialization attack because phar: is blocked but PHAR: is not blocked.
CVE-2020-28949	Archive_Tar through 1.4.10 has ::// filename sanitization only to address phar attacks, and thus any other stream-wrapper attack (such as file:// to overwrite files) can still succeed.
CVE-2020-28974	A slab-out-of-bounds read in fbcon in the Linux kernel before 5.9.7 could be used by local attackers to read privileged information or potentially crash the kernel, aka CID-3c4e0dff2095. This occurs because KD_FONT_OP_COPY in drivers/tty/vt/vt.c can be used for manipulations such as font height.
CVE-2020-29129	ncsi.c in libslirp through 4.3.1 has a buffer over-read because it tries to read a certain amount of header data even if that exceeds the total packet length.
CVE-2020-29130	slirp.c in libslirp through 4.3.1 has a buffer over-read because it tries to read a certain amount of header data even if that exceeds the total packet length.
CVE-2020-2922	Vulnerability in the MySQL Client product of Oracle MySQL (component: C API). Supported versions that are affected are 5.6.47 and prior, 5.7.29 and prior and 8.0.18 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Client accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2020-29361	An issue was discovered in p11-kit 0.21.1 through 0.23.21. Multiple integer overflows have been discovered in the array allocations in the p11-kit library and the p11-kit list command, where overflow checks are missing before calling realloc or calloc.
CVE-2020-29362	An issue was discovered in p11-kit 0.21.1 through 0.23.21. A heap-based buffer over-read has been discovered in the RPC protocol used by the p11-kit server/remote commands and the client library. When the remote entity supplies a byte array through a serialized PKCS#11 function call, the receiving entity may allow the reading of up to 4 bytes of memory past the heap allocation.
CVE-2020-29363	An issue was discovered in p11-kit 0.23.6 through 0.23.21. A heap-based buffer overflow has been discovered in the RPC protocol used by p11-kit server/remote commands and the client library. When the remote entity supplies a serialized byte array in a CK_ATTRIBUTE, the receiving entity may not allocate

	sufficient length for the buffer to store the deserialized value.
CVE-2020-29374	An issue was discovered in the Linux kernel before 5.7.3, related to mm/gup.c and mm/huge_memory.c. The get_user_pages (aka gup) implementation, when used for a copy-on-write page, does not properly consider the semantics of read operations and therefore can grant unintended write access, aka CID-17839856fd58.
CVE-2020-29443	ide_atapi_cmd_reply_end in hw/ide/atapi.c in QEMU 5.1.0 allows out-of-bounds read access because a buffer index is not validated.
CVE-2020-29444	Affected versions of Team Calendar in Confluence Server before 7.11.0 allow attackers to inject arbitrary HTML or Javascript via a Cross Site Scripting Vulnerability in admin global setting parameters.
CVE-2020-29445	Affected versions of Confluence Server before 7.4.8, and versions from 7.5.0 before 7.11.0 allow attackers to identify internal hosts and ports via a blind server-side request forgery vulnerability in Team Calendars parameters.
CVE-2020-29448	The ConfluenceResourceDownloadRewriteRule class in Confluence Server and Confluence Data Center before version 6.13.18, from 6.14.0 before 7.4.6, and from 7.5.0 before 7.8.3 allowed unauthenticated remote attackers to read arbitrary files within WEB-INF and META-INF directories via an incorrect path access check.
CVE-2020-29450	Affected versions of Atlassian Confluence Server and Data Center allow remote attackers to impact the application's availability via a Denial of Service (DoS) vulnerability in the avatar upload feature. The affected versions are before version 7.2.0.
CVE-2020-29562	The iconv function in the GNU C Library (aka glibc or libc6) 2.30 to 2.32, when converting UCS4 text containing an irreversible character, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.
CVE-2020-29568	An issue was discovered in Xen through 4.14.x. Some OSes (such as Linux, FreeBSD, and NetBSD) are processing watch events using a single thread. If the events are received faster than the thread is able to handle, they will get queued. As the queue is unbounded, a guest may be able to trigger an OOM in the backend. All systems with a FreeBSD, Linux, or NetBSD (any version) dom0 are vulnerable.
CVE-2020-29569	An issue was discovered in the Linux kernel through 5.10.1, as used with Xen through 4.14.x. The Linux kernel PV block backend expects the kernel thread handler to reset ring->xenblk to NULL when stopped.

	However, the handler may not have time to run if the frontend quickly toggles between the states connect and disconnect. As a consequence, the block backend may re-use a pointer after it was freed. A misbehaving guest can trigger a dom0 crash by continuously connecting / disconnecting a block frontend. Privilege escalation and information leaks cannot be ruled out. This only affects systems with a Linux blkback.
CVE-2020-29599	ImageMagick before 6.9.11-40 and 7.x before 7.0.10-40 mishandles the -authenticate option, which allows setting a password for password-protected PDF files. The user-controlled password was not properly escaped/sanitized and it was therefore possible to inject additional shell commands via coders/pdf.c.
CVE-2020-29652	A nil pointer dereference in the golang.org/x/crypto/ssh component through v0.0.0-20201203163018-be400aefbc4c for Go allows remote attackers to cause a denial of service against SSH servers.
CVE-2020-29660	A locking inconsistency issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_io.c and drivers/tty/tty_jobctrl.c may allow a read-after-free attack against TIOCGSID, aka CID-c8bcd9c5be24.
CVE-2020-29661	A locking issue was discovered in the tty subsystem of the Linux kernel through 5.9.13. drivers/tty/tty_jobctrl.c allows a use-after-free attack against TIOCSPGRP, aka CID-54ffccbf053b.
CVE-2020-2968	Vulnerability in the Java VM component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows low privileged attacker having Create Session, Create Procedure privilege with network access via multiple protocols to compromise Java VM. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java VM, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java VM. CVSS 3.1 Base Score 8.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H).
CVE-2020-2969	Vulnerability in the Data Pump component of Oracle Database Server. Supported versions that are affected are 11.2.0.4, 12.1.0.2, 12.2.0.1, 18c and 19c. Difficult to exploit vulnerability allows high privileged attacker having DBA role account privilege with network access via Oracle Net to compromise Data Pump. Successful attacks of this vulnerability can result in takeover of Data Pump. CVSS 3.1 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).

CVE-2020-2978	Vulnerability in the Oracle Database - Enterprise Edition component of Oracle Database Server. Supported versions that are affected are 12.1.0.2, 12.2.0.1, 18c and 19c. Easily exploitable vulnerability allows high privileged attacker having DBA role account privilege with network access via Oracle Net to compromise Oracle Database - Enterprise Edition. While the vulnerability is in Oracle Database - Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Database - Enterprise Edition accessible data. CVSS 3.1 Base Score 4.1 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:L/A:N).
CVE-2020-35111	When an extension with the proxy permission registered to receive <all_urls>, the proxy.onRequest callback was not triggered for view-source URLs. While web content cannot navigate to such URLs, a user opening View Source could have inadvertently leaked their IP address. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.
CVE-2020-35113	Mozilla developers reported memory safety bugs present in Firefox 83 and Firefox ESR 78.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 84, Thunderbird < 78.6, and Firefox ESR < 78.6.
CVE-2020-35448	An issue was discovered in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.35.1. A heap-based buffer over-read can occur in bfd_getl_signed_32 in libbfd.c because sh_entsize is not validated in _bfd_elf_slurp_secondary_reloc_section in elf.c.
CVE-2020-35452	Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Digest nonce can cause a stack overflow in mod_auth_digest. There is no report of this overflow being exploitable, nor the Apache HTTP Server team could create one, though some particular compiler and/or compilation option might make it possible, with limited consequences anyway due to the size (a single byte) and the value (zero byte) of the overflow
CVE-2020-35518	When binding against a DN during authentication, the reply from 389-ds-base will be different whether the DN exists or not. This can be used by an unauthenticated attacker to check the existence of an entry in the LDAP database.

CVE-2020-35521	A flaw was found in libtiff. Due to a memory allocation failure in tif_read.c, a crafted TIFF file can lead to an abort, resulting in denial of service.
CVE-2020-35522	In LibTIFF, there is a memory malloc failure in tif_pixmaplog.c. A crafted TIFF document can lead to an abort, resulting in a remote denial of service attack.
CVE-2020-35523	An integer overflow flaw was found in libtiff that exists in the tif_gettime.c file. This flaw allows an attacker to inject and execute arbitrary code when a user opens a crafted TIFF file. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2020-35524	A heap-based buffer overflow flaw was found in libtiff in the handling of TIFF images in libtiff's TIFF2PDF tool. A specially crafted TIFF file can lead to arbitrary code execution. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2020-36193	Tar.php in Archive_Tar through 1.4.11 allows write operations with Directory Traversal due to inadequate checking of symbolic links, a related issue to CVE-2020-28948.
CVE-2020-36225	A flaw was discovered in OpenLDAP before 2.4.57 leading to a double free and slapd crash in the saslAuthzTo processing, resulting in denial of service.
CVE-2020-36311	An issue was discovered in the Linux kernel before 5.9. arch/x86/kvm/svm/sev.c allows attackers to cause a denial of service (soft lockup) by triggering destruction of a large SEV VM (which requires unregistering many encrypted regions), aka CID-7be74942f184.
CVE-2020-36322	An issue was discovered in the FUSE filesystem implementation in the Linux kernel before 5.10.6, aka CID-5d069dbe8aaf. fuse_do_getattr() calls make_bad_inode() in inappropriate situations, causing a system crash. NOTE: the original fix for this vulnerability was incomplete, and its incompleteness is tracked as CVE-2021-28950.
CVE-2020-36323	In the standard library in Rust before 1.52.0, there is an optimization for joining strings that can cause uninitialized bytes to be exposed (or the program to crash) if the borrowed string changes after its length is checked.
CVE-2020-36328	A flaw was found in libwebp in versions before 1.0.1. A heap-based buffer overflow in function WebPDecodeRGBInto is possible due to an invalid check for buffer size. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-36329	A flaw was found in libwebp in versions before 1.0.1. A use-after-free was found due to a thread being killed

	too early. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2020-3702	u'Specifically timed and handcrafted traffic can cause internal errors in a WLAN device that lead to improper layer 2 Wi-Fi encryption with a consequent possibility of information disclosure over the air for a discrete set of traffic' in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, IPQ4019, IPQ8064, MSM8909W, MSM8996AU, QCA9531, QCN5502, QCS405, SDX20, SM6150, SM7150
CVE-2020-3757	Adobe Flash Player versions 32.0.0.321 and earlier, 32.0.0.314 and earlier, 32.0.0.321 and earlier, and 32.0.0.255 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2020-3862	A denial of service issue was addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. A malicious website may be able to cause a denial of service.
CVE-2020-3864	A logic issue was addressed with improved validation. This issue is fixed in iCloud for Windows 7.17, iTunes 12.10.4 for Windows, iCloud for Windows 10.9.2, tvOS 13.3.1, Safari 13.0.5, iOS 13.3.1 and iPadOS 13.3.1. A DOM object context may not have had a unique security origin.
CVE-2020-3865	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2020-3867	A logic issue was addressed with improved state management. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing maliciously crafted web content may lead to universal cross site scripting.
CVE-2020-3868	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in iOS 13.3.1 and iPadOS 13.3.1, tvOS 13.3.1, Safari 13.0.5, iTunes for Windows 12.10.4, iCloud for Windows 11.0, iCloud for Windows 7.17. Processing

	maliciously crafted web content may lead to arbitrary code execution.
CVE-2020-3885	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A file URL may be incorrectly processed.
CVE-2020-3894	A race condition was addressed with additional validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. An application may be able to read restricted memory.
CVE-2020-3895	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2020-3897	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution.
CVE-2020-3899	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. A remote attacker may be able to cause arbitrary code execution.
CVE-2020-3900	A memory corruption issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2020-3901	A type confusion issue was addressed with improved memory handling. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, watchOS 6.2, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud for Windows 7.18. Processing maliciously crafted web content may lead to arbitrary code execution.
CVE-2020-3902	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 13.4 and iPadOS 13.4, tvOS 13.4, Safari 13.1, iTunes for Windows 12.10.5, iCloud for Windows 10.9.3, iCloud

	for Windows 7.18. Processing maliciously crafted web content may lead to a cross site scripting attack.
CVE-2020-4006	VMware Workspace One Access, Access Connector, Identity Manager, and Identity Manager Connector address have a command injection vulnerability.
CVE-2020-4027	Affected versions of Atlassian Confluence Server and Data Center allowed remote attackers with system administration permissions to bypass velocity template injection mitigations via an injection vulnerability in custom user macros. The affected versions are before version 7.4.5, and from version 7.5.0 before 7.5.1.
CVE-2020-4163	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0, under specialized conditions, could allow an authenticated user to create a maliciously crafted file name which would be misinterpreted as jsp content and executed. IBM X-Force ID: 174397.
CVE-2020-4276	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional is vulnerable to a privilege escalation vulnerability when using token-based authentication in an admin request over the SOAP connector. X-Force ID: 175984.
CVE-2020-4329	IBM WebSphere Application Server 7.0, 8.0, 8.5, 9.0 and Liberty 17.0.0.3 through 20.0.0.4 could allow a remote, authenticated attacker to obtain sensitive information, caused by improper parameter checking. This could be exploited to conduct spoofing attacks. IBM X-Force ID: 177841.
CVE-2020-4362	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional is vulnerable to a privilege escalation vulnerability when using token-based authentication in an admin request over the SOAP connector. IBM X-Force ID: 178929.
CVE-2020-4365	IBM WebSphere Application Server 8.5 is vulnerable to server-side request forgery. By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 178964.
CVE-2020-4448	IBM WebSphere Application Server Network Deployment 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects from untrusted sources. IBM X-Force ID: 181228.
CVE-2020-4449	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional could allow a remote attacker to obtain sensitive information with a specially-crafted sequence of serialized objects. IBM X-Force ID: 181230.
CVE-2020-4450	IBM WebSphere Application Server 8.5 and 9.0 traditional could allow a remote attacker to execute arbitrary code on the system with a specially-crafted

	sequence of serialized objects. IBM X-Force ID: 181231.
CVE-2020-4464	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional could allow a remote attacker to execute arbitrary code on a system with a specially-crafted sequence of serialized objects over the SOAP connector. IBM X-Force ID: 181489.
CVE-2020-4534	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a local authenticated attacker to gain elevated privileges on the system, caused by improper handling of UNC paths. By scheduling a task with a specially-crafted UNC path, an attacker could exploit this vulnerability to execute arbitrary code with higher privileges. IBM X-Force ID: 182808.
CVE-2020-4575	IBM WebSphere Application Server ND 8.5 and 9.0, and IBM WebSphere Virtual Enterprise 7.0 and 8.0 are vulnerable to cross-site scripting when High Availability Deployment Manager is configured.
CVE-2020-4578	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 184433.
CVE-2020-4589	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 could allow a remote attacker to execute arbitrary code on the system with a specially-crafted sequence of serialized objects from untrusted sources. IBM X-Force ID: 184585.
CVE-2020-4643	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information. IBM X-Force ID: 185590.
CVE-2020-4945	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 could allow an authenticated user to overwrite arbitrary files due to improper group permissions. IBM X-Force ID: 191945.
CVE-2020-4949	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 192025.
CVE-2020-5208	It's been found that multiple functions in ipmitool before 1.8.19 neglect proper checking of the data received from a remote LAN party, which may lead to buffer overflows and potentially to remote code execution on the ipmitool side. This is especially dangerous if

	ipmitool is run as a privileged user. This problem is fixed in version 1.8.19.
CVE-2020-5260	Affected versions of Git have a vulnerability whereby Git can be tricked into sending private credentials to a host controlled by an attacker. Git uses external "credential helper" programs to store and retrieve passwords or other credentials from secure storage provided by the operating system. Specially-crafted URLs that contain an encoded newline can inject unintended values into the credential helper protocol stream, causing the credential helper to retrieve the password for one server (e.g., good.example.com) for an HTTP request being made to another server (e.g., evil.example.com), resulting in credentials for the former being sent to the latter. There are no restrictions on the relationship between the two, meaning that an attacker can craft a URL that will present stored credentials for any host to a host of their choosing. The vulnerability can be triggered by feeding a malicious URL to git clone. However, the affected URLs look rather suspicious; the likely vector would be through systems which automatically clone URLs not visible to the user, such as Git submodules, or package systems built around Git. The problem has been patched in the versions published on April 14th, 2020, going back to v2.17.x. Anyone wishing to backport the change further can do so by applying commit 9a6bbee (the full release includes extra checks for git fsck, but that commit is sufficient to protect clients against the vulnerability). The patched versions are: 2.17.4, 2.18.3, 2.19.4, 2.20.3, 2.21.2, 2.22.3, 2.23.2, 2.24.2, 2.25.3, 2.26.1.
CVE-2020-5312	libImaging/PcxDecode.c in Pillow before 6.2.2 has a PCX P mode buffer overflow.
CVE-2020-5313	libImaging/FliDecode.c in Pillow before 6.2.2 has an FLI buffer overflow.
CVE-2020-5395	FontForge 20190801 has a use-after-free in SFD_GetFontMetaData in sfd.c.
CVE-2020-6096	An exploitable signed comparison vulnerability exists in the ARMv7 memcpy() implementation of GNU glibc 2.30.9000. Calling memcpy() (on ARMv7 targets that utilize the GNU glibc implementation) with a negative value for the 'num' parameter results in a signed comparison vulnerability. If an attacker underflows the 'num' parameter to memcpy(), this vulnerability could lead to undefined behavior such as writing to out-of-bounds memory and potentially remote code execution. Furthermore, this memcpy() implementation allows for program execution to continue in scenarios where a segmentation fault or crash should have occurred. The dangers occur in that subsequent execution

	and iterations of this code will be executed with this corrupted data.
CVE-2020-6377	Use after free in audio in Google Chrome prior to 79.0.3945.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6378	Use after free in speech in Google Chrome prior to 79.0.3945.130 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6379	Use after free in V8 in Google Chrome prior to 79.0.3945.130 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6380	Insufficient policy enforcement in extensions in Google Chrome prior to 79.0.3945.130 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted Chrome Extension.
CVE-2020-6381	Integer overflow in JavaScript in Google Chrome on ChromeOS and Android prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6382	Type confusion in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6383	Type confusion in V8 in Google Chrome prior to 80.0.3987.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6384	Use after free in WebAudio in Google Chrome prior to 80.0.3987.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6385	Insufficient policy enforcement in storage in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2020-6386	Use after free in speech in Google Chrome prior to 80.0.3987.116 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6387	Out of bounds write in WebRTC in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted video stream.
CVE-2020-6388	Out of bounds access in WebAudio in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6389	Out of bounds write in WebRTC in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted video stream.
CVE-2020-6390	Out of bounds memory access in streams in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2020-6391	Insufficient validation of untrusted input in Blink in Google Chrome prior to 80.0.3987.87 allowed a local attacker to bypass content security policy via a crafted HTML page.
CVE-2020-6392	Insufficient policy enforcement in extensions in Google Chrome prior to 80.0.3987.87 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.
CVE-2020-6393	Insufficient policy enforcement in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6394	Insufficient policy enforcement in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2020-6395	Out of bounds read in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-6396	Inappropriate implementation in Skia in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-6397	Inappropriate implementation in sharing in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-6398	Use of uninitialized data in PDFium in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2020-6399	Insufficient policy enforcement in AppCache in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6400	Inappropriate implementation in CORS in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6401	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2020-6402	Insufficient policy enforcement in downloads in Google Chrome on OS X prior to 80.0.3987.87 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension.
CVE-2020-6403	Incorrect implementation in Omnibox in Google Chrome on iOS prior to 80.0.3987.87 allowed a remote attacker

	to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-6404	Inappropriate implementation in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6405	Out of bounds read in SQLite in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-6406	Use after free in audio in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6407	Out of bounds memory access in streams in Google Chrome prior to 80.0.3987.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6408	Insufficient policy enforcement in CORS in Google Chrome prior to 80.0.3987.87 allowed a local attacker to obtain potentially sensitive information via a crafted HTML page.
CVE-2020-6409	Inappropriate implementation in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker who convinced the user to enter a URI to bypass navigation restrictions via a crafted domain name.
CVE-2020-6410	Insufficient policy enforcement in navigation in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to confuse the user via a crafted domain name.
CVE-2020-6411	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2020-6412	Insufficient validation of untrusted input in Omnibox in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2020-6413	Inappropriate implementation in Blink in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass HTML validators via a crafted HTML page.
CVE-2020-6414	Insufficient policy enforcement in Safe Browsing in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6415	Inappropriate implementation in JavaScript in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2020-6416	Insufficient data validation in streams in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6417	Inappropriate implementation in installer in Google Chrome prior to 80.0.3987.87 allowed a local attacker to execute arbitrary code via a crafted registry entry.
CVE-2020-6418	Type confusion in V8 in Google Chrome prior to 80.0.3987.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6419	Out of bounds write in V8 in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6420	Insufficient policy enforcement in media in Google Chrome prior to 80.0.3987.132 allowed a remote attacker to bypass same origin policy via a crafted HTML page.
CVE-2020-6422	Use after free in WebGL in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6423	Use after free in audio in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6424	Use after free in media in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6425	Insufficient policy enforcement in extensions in Google Chrome prior to 80.0.3987.149 allowed an attacker who convinced a user to install a malicious extension to bypass site isolation via a crafted Chrome Extension.
CVE-2020-6426	Inappropriate implementation in V8 in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6427	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6428	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6429	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6430	Type Confusion in V8 in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2020-6431	Insufficient policy enforcement in full screen in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-6432	Insufficient policy enforcement in navigations in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6433	Insufficient policy enforcement in extensions in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6434	Use after free in devtools in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6435	Insufficient policy enforcement in extensions in Google Chrome prior to 81.0.4044.92 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6436	Use after free in window management in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6437	Inappropriate implementation in WebView in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to spoof security UI via a crafted application.
CVE-2020-6438	Insufficient policy enforcement in extensions in Google Chrome prior to 81.0.4044.92 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory via a crafted Chrome Extension.
CVE-2020-6439	Insufficient policy enforcement in navigations in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass security UI via a crafted HTML page.
CVE-2020-6440	Inappropriate implementation in extensions in Google Chrome prior to 81.0.4044.92 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information via a crafted Chrome Extension.
CVE-2020-6441	Insufficient policy enforcement in omnibox in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass security UI via a crafted HTML page.
CVE-2020-6442	Inappropriate implementation in cache in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6443	Insufficient data validation in developer tools in Google Chrome prior to 81.0.4044.92 allowed a remote attacker who had convinced the user to use devtools to execute arbitrary code via a crafted HTML page.

CVE-2020-6444	Uninitialized use in WebRTC in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6445	Insufficient policy enforcement in trusted types in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2020-6446	Insufficient policy enforcement in trusted types in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2020-6447	Inappropriate implementation in developer tools in Google Chrome prior to 81.0.4044.92 allowed a remote attacker who had convinced the user to use devtools to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6448	Use after free in V8 in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6449	Use after free in audio in Google Chrome prior to 80.0.3987.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6450	Use after free in WebAudio in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6451	Use after free in WebAudio in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6452	Heap buffer overflow in media in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6453	Inappropriate implementation in V8 in Google Chrome prior to 80.0.3987.162 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6454	Use after free in extensions in Google Chrome prior to 81.0.4044.92 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2020-6455	Out of bounds read in WebSQL in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6456	Insufficient validation of untrusted input in clipboard in Google Chrome prior to 81.0.4044.92 allowed a local attacker to bypass site isolation via crafted clipboard contents.

CVE-2020-6457	Use after free in speech recognizer in Google Chrome prior to 81.0.4044.113 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6458	Out of bounds read and write in PDFium in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2020-6459	Use after free in payments in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6460	Insufficient data validation in URL formatting in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to perform domain spoofing via a crafted domain name.
CVE-2020-6461	Use after free in storage in Google Chrome prior to 81.0.4044.129 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6462	Use after free in task scheduling in Google Chrome prior to 81.0.4044.129 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6463	Use after free in ANGLE in Google Chrome prior to 81.0.4044.122 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6464	Type confusion in Blink in Google Chrome prior to 81.0.4044.138 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6465	Use after free in reader mode in Google Chrome on Android prior to 83.0.4103.61 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6466	Use after free in media in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6467	Use after free in WebRTC in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6468	Type confusion in V8 in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6469	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious

	extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2020-6470	Insufficient validation of untrusted input in clipboard in Google Chrome prior to 83.0.4103.61 allowed a local attacker to inject arbitrary scripts or HTML (UXSS) via crafted clipboard contents.
CVE-2020-6471	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2020-6472	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from process memory or disk via a crafted Chrome Extension.
CVE-2020-6473	Insufficient policy enforcement in Blink in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-6474	Use after free in Blink in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6475	Incorrect implementation in full screen in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-6476	Insufficient policy enforcement in tab strip in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.
CVE-2020-6477	Inappropriate implementation in installer in Google Chrome on OS X prior to 83.0.4103.61 allowed a local attacker to perform privilege escalation via a crafted file.
CVE-2020-6478	Inappropriate implementation in full screen in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-6479	Inappropriate implementation in sharing in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-6480	Insufficient policy enforcement in enterprise in Google Chrome prior to 83.0.4103.61 allowed a local attacker to bypass navigation restrictions via UI actions.
CVE-2020-6481	Insufficient policy enforcement in URL formatting in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to perform domain spoofing via a crafted domain name.

CVE-2020-6482	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.61 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.
CVE-2020-6483	Insufficient policy enforcement in payments in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6484	Insufficient data validation in ChromeDriver in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted request.
CVE-2020-6485	Insufficient data validation in media router in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6486	Insufficient policy enforcement in navigations in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6487	Insufficient policy enforcement in downloads in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6488	Insufficient policy enforcement in downloads in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6489	Inappropriate implementation in developer tools in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had convinced the user to take certain actions in developer tools to obtain potentially sensitive information from disk via a crafted HTML page.
CVE-2020-6490	Insufficient data validation in loader in Google Chrome prior to 83.0.4103.61 allowed a remote attacker who had been able to write to disk to leak cross-origin data via a crafted HTML page.
CVE-2020-6491	Insufficient data validation in site information in Google Chrome prior to 83.0.4103.61 allowed a remote attacker to spoof security UI via a crafted domain name.
CVE-2020-6492	Use after free in ANGLE in Google Chrome prior to 83.0.4103.97 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6493	Use after free in WebAuthentication in Google Chrome prior to 83.0.4103.97 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6494	Incorrect security UI in payments in Google Chrome on Android prior to 83.0.4103.97 allowed a remote attacker

	to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-6495	Insufficient policy enforcement in developer tools in Google Chrome prior to 83.0.4103.97 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2020-6496	Use after free in payments in Google Chrome on MacOS prior to 83.0.4103.97 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6499	Inappropriate implementation in AppCache in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass AppCache security restrictions via a crafted HTML page.
CVE-2020-6500	Inappropriate implementation in interstitials in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-6501	Insufficient policy enforcement in CSP in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2020-6502	Incorrect implementation in permissions in Google Chrome prior to 80.0.3987.87 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2020-6503	Inappropriate implementation in accessibility in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-6504	Insufficient policy enforcement in notifications in Google Chrome prior to 74.0.3729.108 allowed a remote attacker to bypass notification restrictions via a crafted HTML page.
CVE-2020-6505	Use after free in speech in Google Chrome prior to 83.0.4103.106 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6506	Insufficient policy enforcement in WebView in Google Chrome on Android prior to 83.0.4103.106 allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2020-6507	Out of bounds write in V8 in Google Chrome prior to 83.0.4103.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6509	Use after free in extensions in Google Chrome prior to 83.0.4103.116 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.

CVE-2020-6510	Heap buffer overflow in background fetch in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6511	Information leak in content security policy in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6512	Type Confusion in V8 in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6513	Heap buffer overflow in PDFium in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2020-6514	Inappropriate implementation in WebRTC in Google Chrome prior to 84.0.4147.89 allowed an attacker in a privileged network position to potentially exploit heap corruption via a crafted SCTP stream.
CVE-2020-6515	Use after free in tab strip in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6516	Policy bypass in CORS in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6517	Heap buffer overflow in history in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6518	Use after free in developer tools in Google Chrome prior to 84.0.4147.89 allowed a remote attacker who had convinced the user to use developer tools to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6519	Policy bypass in CSP in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2020-6520	Buffer overflow in Skia in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6521	Side-channel information leakage in autofill in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-6522	Inappropriate implementation in external protocol handlers in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6523	Out of bounds write in Skia in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2020-6524	Heap buffer overflow in WebAudio in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6525	Heap buffer overflow in Skia in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6526	Inappropriate implementation in iframe sandbox in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6527	Insufficient policy enforcement in CSP in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2020-6528	Incorrect security UI in basic auth in Google Chrome on iOS prior to 84.0.4147.89 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-6529	Inappropriate implementation in WebRTC in Google Chrome prior to 84.0.4147.89 allowed an attacker in a privileged network position to leak cross-origin data via a crafted HTML page.
CVE-2020-6530	Out of bounds memory access in developer tools in Google Chrome prior to 84.0.4147.89 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2020-6531	Side-channel information leakage in scroll to text in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6532	Use after free in SCTP in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6533	Type Confusion in V8 in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6534	Heap buffer overflow in WebRTC in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6535	Insufficient data validation in WebUI in Google Chrome prior to 84.0.4147.89 allowed a remote attacker who had compromised the renderer process to inject scripts or HTML into a privileged page via a crafted HTML page.
CVE-2020-6536	Incorrect security UI in PWAs in Google Chrome prior to 84.0.4147.89 allowed a remote attacker who had

	persuaded the user to install a PWA to spoof the contents of the Omnibox (URL bar) via a crafted PWA.
CVE-2020-6537	Type confusion in V8 in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2020-6538	Inappropriate implementation in WebView in Google Chrome on Android prior to 84.0.4147.105 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6539	Use after free in CSS in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6540	Buffer overflow in Skia in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6541	Use after free in WebUSB in Google Chrome prior to 84.0.4147.105 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6542	Use after free in ANGLE in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6543	Use after free in task scheduling in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6544	Use after free in media in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6545	Use after free in audio in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6546	Inappropriate implementation in installer in Google Chrome prior to 84.0.4147.125 allowed a local attacker to potentially elevate privilege via a crafted filesystem.
CVE-2020-6547	Incorrect security UI in media in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially obtain sensitive information via a crafted HTML page.
CVE-2020-6548	Heap buffer overflow in Skia in Google Chrome prior to 84.0.4147.125 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6549	Use after free in media in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6550	Use after free in IndexedDB in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2020-6551	Use after free in WebXR in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6552	Use after free in Blink in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6553	Use after free in offline mode in Google Chrome on iOS prior to 84.0.4147.125 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6554	Use after free in extensions in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2020-6555	Out of bounds read in WebGL in Google Chrome prior to 84.0.4147.125 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2020-6556	Heap buffer overflow in SwiftShader in Google Chrome prior to 84.0.4147.135 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6557	Inappropriate implementation in networking in Google Chrome prior to 86.0.4240.75 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2020-6559	Use after free in presentation API in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6560	Insufficient policy enforcement in autofill in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6561	Inappropriate implementation in Content Security Policy in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6562	Insufficient policy enforcement in Blink in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6563	Insufficient policy enforcement in intent handling in Google Chrome on Android prior to 85.0.4183.83 allowed a remote attacker to obtain potentially sensitive information from disk via a crafted HTML page.
CVE-2020-6564	Inappropriate implementation in permissions in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to spoof the contents of a permission dialog via a crafted HTML page.

CVE-2020-6565	Inappropriate implementation in Omnibox in Google Chrome on iOS prior to 85.0.4183.83 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2020-6566	Insufficient policy enforcement in media in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2020-6567	Insufficient validation of untrusted input in command line handling in Google Chrome on Windows prior to 85.0.4183.83 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6568	Insufficient policy enforcement in intent handling in Google Chrome on Android prior to 85.0.4183.83 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2020-6569	Integer overflow in WebUSB in Google Chrome prior to 85.0.4183.83 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6570	Information leakage in WebRTC in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to obtain potentially sensitive information via a crafted WebRTC interaction.
CVE-2020-6571	Insufficient data validation in Omnibox in Google Chrome prior to 85.0.4183.83 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2020-6572	Use after free in Media in Google Chrome prior to 81.0.4044.92 allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2020-6573	Use after free in video in Google Chrome on Android prior to 85.0.4183.102 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6574	Insufficient policy enforcement in installer in Google Chrome on OS X prior to 85.0.4183.102 allowed a local attacker to potentially achieve privilege escalation via a crafted binary.
CVE-2020-6575	Race in Mojo in Google Chrome prior to 85.0.4183.102 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2020-6576	Use after free in offscreen canvas in Google Chrome prior to 85.0.4183.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2020-6792	When deriving an identifier for an email message, uninitialized memory was used in addition to

	the message contents. This vulnerability affects Thunderbird < 68.5.
CVE-2020-6793	When processing an email message with an ill-formed envelope, Thunderbird could read data from a random memory location. This vulnerability affects Thunderbird < 68.5.
CVE-2020-6794	If a user saved passwords before Thunderbird 60 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 Thunderbird 60. 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 Thunderbird < 68.5.
CVE-2020-6795	When processing a message that contains multiple S/MIME signatures, a bug in the MIME processing code caused a null pointer dereference, leading to an unexploitable crash. This vulnerability affects Thunderbird < 68.5.
CVE-2020-6798	If a template tag was used in a select tag, the parser could be confused and allow JavaScript parsing and execution when it should not be allowed. A site that relied on the browser behaving correctly could suffer a cross-site scripting vulnerability as a result. In general, this flaw cannot be exploited through email in the Thunderbird product because scripting is disabled when reading mail, but is potentially a risk in browser or browser-like contexts. This vulnerability affects Thunderbird < 68.5, Firefox < 73, and Firefox < ESR68.5.
CVE-2020-6800	Mozilla developers and community members reported memory safety bugs present in Firefox 72 and Firefox ESR 68.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. In general, these flaws cannot be exploited through email in the Thunderbird product because scripting is disabled when reading mail, but are potentially risks in browser or browser-like contexts. This vulnerability affects Thunderbird < 68.5, Firefox < 73, and Firefox < ESR68.5.
CVE-2020-6805	When removing data about an origin whose tab was recently closed, a use-after-free could occur in the Quota manager, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6.
CVE-2020-6806	By carefully crafting promise resolutions, it was possible to cause an out-of-bounds read off the end of an array resized during script execution. This could have led to

	memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6.
CVE-2020-6807	When a device was changed while a stream was about to be destroyed, the <code><code>stream-reinit</code></code> task may have been executed after the stream was destroyed, causing a use-after-free and a potentially exploitable crash. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6.
CVE-2020-6811	The 'Copy as cURL' feature of Devtools' network tab did not properly escape the HTTP method of a request, which can be controlled by the website. If a user used the 'Copy as Curl' feature and pasted the command into a terminal, it could have resulted in command injection and arbitrary command execution. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6.
CVE-2020-6812	The first time AirPods are connected to an iPhone, they become named after the user's name by default (e.g. Jane Doe's AirPods.) Websites with camera or microphone permission are able to enumerate device names, disclosing the user's name. To resolve this issue, Firefox added a special case that renames devices containing the substring 'AirPods' to simply 'AirPods'. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6.
CVE-2020-6814	Mozilla developers reported memory safety bugs present in Firefox and Thunderbird 68.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.6, Firefox < 74, Firefox < ESR68.6, and Firefox ESR < 68.6.
CVE-2020-6819	Under certain conditions, when running the nsDocShell destructor, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.
CVE-2020-6820	Under certain conditions, when handling a ReadableStream, a race condition can cause a use-after-free. We are aware of targeted attacks in the wild abusing this flaw. This vulnerability affects Thunderbird < 68.7.0, Firefox < 74.0.1, and Firefox ESR < 68.6.1.
CVE-2020-6821	When reading from areas partially or fully outside the source resource with WebGL's <code><code>copyTexSubImage</code></code> method, the specification requires the returned values be zero. Previously, this memory was uninitialized, leading to potentially sensitive data disclosure. This vulnerability

	affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.
CVE-2020-6822	On 32-bit builds, an out of bounds write could have occurred when processing an image larger than 4 GB in <code><code>GMPDecodeData</code></code> . It is possible that with enough effort this could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.
CVE-2020-6825	Mozilla developers and community members Tyson Smith and Christian Holler reported memory safety bugs present in Firefox 74 and Firefox ESR 68.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 68.7.0, Firefox ESR < 68.7, and Firefox < 75.
CVE-2020-6829	When performing EC scalar point multiplication, the wNAF point multiplication algorithm was used; which leaked partial information about the nonce used during signature generation. Given an electro-magnetic trace of a few signature generations, the private key could have been computed. This vulnerability affects Firefox < 80 and Firefox for Android < 80.
CVE-2020-6831	A buffer overflow could occur when parsing and validating SCTP chunks in WebRTC. This could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox ESR < 68.8, Firefox < 76, and Thunderbird < 68.8.0.
CVE-2020-7009	Elasticsearch versions from 6.7.0 before 6.8.8 and 7.0.0 before 7.6.2 contain a privilege escalation flaw if an attacker is able to create API keys. An attacker who is able to generate an API key can perform a series of steps that result in an API key being generated with elevated privileges.
CVE-2020-7012	Kibana versions 6.7.0 to 6.8.8 and 7.0.0 to 7.6.2 contain a prototype pollution flaw in the Upgrade Assistant. An authenticated attacker with privileges to write to the Kibana index could insert data that would cause Kibana to execute arbitrary code. This could possibly lead to an attacker executing code with the permissions of the Kibana process on the host system.
CVE-2020-7013	Kibana versions before 6.8.9 and 7.7.0 contain a prototype pollution flaw in TSVB. An authenticated attacker with privileges to create TSVB visualizations could insert data that would cause Kibana to execute arbitrary code. This could possibly lead to an attacker executing code with the permissions of the Kibana process on the host system.
CVE-2020-7014	The fix for CVE-2020-7009 was found to be incomplete. Elasticsearch versions from 6.7.0 to 6.8.7 and 7.0.0 to

	7.6.1 contain a privilege escalation flaw if an attacker is able to create API keys and also authentication tokens. An attacker who is able to generate an API key and an authentication token can perform a series of steps that result in an authentication token being generated with elevated privileges.
CVE-2020-7015	Kibana versions before 6.8.9 and 7.7.0 contains a stored XSS flaw in the TSVB visualization. An attacker who is able to edit or create a TSVB visualization could allow the attacker to obtain sensitive information from, or perform destructive actions, on behalf of Kibana users who edit the TSVB visualization.
CVE-2020-7016	Kibana versions before 6.8.11 and 7.8.1 contain a denial of service (DoS) flaw in Timelion. An attacker can construct a URL that when viewed by a Kibana user can lead to the Kibana process consuming large amounts of CPU and becoming unresponsive.
CVE-2020-7017	In Kibana versions before 6.8.11 and 7.8.1 the region map visualization contains a stored XSS flaw. An attacker who is able to edit or create a region map visualization could obtain sensitive information or perform destructive actions on behalf of Kibana users who view the region map visualization.
CVE-2020-7019	In Elasticsearch before 7.9.0 and 6.8.12 a field disclosure flaw was found when running a scrolling search with Field Level Security. If a user runs the same query another more privileged user recently ran, the scrolling search can leak fields that should be hidden. This could result in an attacker gaining additional permissions against a restricted index.
CVE-2020-7020	Elasticsearch versions before 6.8.13 and 7.9.2 contain a document disclosure flaw when Document or Field Level Security is used. Search queries do not properly preserve security permissions when executing certain complex queries. This could result in the search disclosing the existence of documents the attacker should not be able to view. This could result in an attacker gaining additional insight into potentially sensitive indices.
CVE-2020-7039	tcp_emu in tcp_subr.c in libslirp 4.1.0, as used in QEMU 4.2.0, mismanages memory, as demonstrated by IRC DCC commands in EMU_IRC. This can cause a heap-based buffer overflow or other out-of-bounds access which can lead to a DoS or potential execute arbitrary code.
CVE-2020-7595	xmlStringLenDecodeEntities in parser.c in libxml2 2.9.10 has an infinite loop in a certain end-of-file situation.
CVE-2020-8112	opj_t1_cblk_decode_processor in openjp2/t1.c in OpenJPEG 2.3.1 through 2020-01-28 has a heap-

	based buffer overflow in the qmfbid==1 case, a different issue than CVE-2020-6851.
CVE-2020-8177	curl 7.20.0 through 7.70.0 is vulnerable to improper restriction of names for files and other resources that can lead too overwriting a local file when the -J flag is used.
CVE-2020-8201	Node.js < 12.18.4 and < 14.11 can be exploited to perform HTTP desync attacks and deliver malicious payloads to unsuspecting users. The payloads can be crafted by an attacker to hijack user sessions, poison cookies, perform clickjacking, and a multitude of other attacks depending on the architecture of the underlying system. The attack was possible due to a bug in processing of carrier-return symbols in the HTTP header names.
CVE-2020-8231	Due to use of a dangling pointer, libcurl 7.29.0 through 7.71.1 can use the wrong connection when sending data.
CVE-2020-8251	Node.js < 14.11.0 is vulnerable to HTTP denial of service (DoS) attacks based on delayed requests submission which can make the server unable to accept new connections.
CVE-2020-8284	A malicious server can use the FTP PASV response to trick curl 7.73.0 and earlier into connecting back to a given IP address and port, and this way potentially make curl extract information about services that are otherwise private and not disclosed, for example doing port scanning and service banner extractions.
CVE-2020-8285	curl 7.21.0 to and including 7.73.0 is vulnerable to uncontrolled recursion due to a stack overflow issue in FTP wildcard match parsing.
CVE-2020-8286	curl 7.41.0 through 7.73.0 is vulnerable to an improper check for certificate revocation due to insufficient verification of the OCSP response.
CVE-2020-8450	An issue was discovered in Squid before 4.10. Due to incorrect buffer management, a remote client can cause a buffer overflow in a Squid instance acting as a reverse proxy.
CVE-2020-8492	Python 2.7 through 2.7.17, 3.5 through 3.5.9, 3.6 through 3.6.10, 3.7 through 3.7.6, and 3.8 through 3.8.1 allows an HTTP server to conduct Regular Expression Denial of Service (ReDoS) attacks against a client because of urllib.request.AbstractBasicAuthHandler catastrophic backtracking.
CVE-2020-8597	eap.c in pppd in ppp 2.4.2 through 2.4.8 has an rhostname buffer overflow in the eap_request and eap_response functions.

CVE-2020-8608	In libslirp 4.1.0, as used in QEMU 4.2.0, tcp_subr.c misuses sprintf return values, leading to a buffer overflow in later code.
CVE-2020-8616	A malicious actor who intentionally exploits this lack of effective limitation on the number of fetches performed when processing referrals can, through the use of specially crafted referrals, cause a recursing server to issue a very large number of fetches in an attempt to process the referral. This has at least two potential effects: The performance of the recursing server can potentially be degraded by the additional work required to perform these fetches, and The attacker can exploit this behavior to use the recursing server as a reflector in a reflection attack with a high amplification factor.
CVE-2020-8617	Using a specially-crafted message, an attacker may potentially cause a BIND server to reach an inconsistent state if the attacker knows (or successfully guesses) the name of a TSIG key used by the server. Since BIND, by default, configures a local session key even on servers whose configuration does not otherwise make use of it, almost all current BIND servers are vulnerable. In releases of BIND dating from March 2018 and after, an assertion check in tsig.c detects this inconsistent state and deliberately exits. Prior to the introduction of the check the server would continue operating in an inconsistent state, with potentially harmful results.
CVE-2020-8622	In BIND 9.0.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.3-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker on the network path for a TSIG-signed request, or operating the server receiving the TSIG-signed request, could send a truncated response to that request, triggering an assertion failure, causing the server to exit. Alternately, an off-path attacker would have to correctly guess when a TSIG-signed request was sent, along with other characteristics of the packet and message, and spoof a truncated response to trigger an assertion failure, causing the server to exit.
CVE-2020-8623	In BIND 9.10.0 -> 9.11.21, 9.12.0 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.10.5-S1 -> 9.11.21-S1 of the BIND 9 Supported Preview Edition, An attacker that can reach a vulnerable system with a specially crafted query packet can trigger a crash. To be vulnerable, the system must: * be running BIND that was built with "--enable-native-pkcs11" * be signing one or more zones with an RSA key * be able to receive queries from a possible attacker
CVE-2020-8624	In BIND 9.9.12 -> 9.9.13, 9.10.7 -> 9.10.8, 9.11.3 -> 9.11.21, 9.12.1 -> 9.16.5, 9.17.0 -> 9.17.3, also affects 9.9.12-S1 -> 9.9.13-S1, 9.11.3-S1 -> 9.11.21-S1 of the

	BIND 9 Supported Preview Edition, An attacker who has been granted privileges to change a specific subset of the zone's content could abuse these unintended additional privileges to update other contents of the zone.
CVE-2020-8625	BIND servers are vulnerable if they are running an affected version and are configured to use GSS-TSIG features. In a configuration which uses BIND's default settings the vulnerable code path is not exposed, but a server can be rendered vulnerable by explicitly setting valid values for the tkey-gssapi-keytab or tkey-gssapi-credentialconfiguration options. Although the default configuration is not vulnerable, GSS-TSIG is frequently used in networks where BIND is integrated with Samba, as well as in mixed-server environments that combine BIND servers with Active Directory domain controllers. The most likely outcome of a successful exploitation of the vulnerability is a crash of the named process. However, remote code execution, while unproven, is theoretically possible. Affects: BIND 9.5.0 -> 9.11.27, 9.12.0 -> 9.16.11, and versions BIND 9.11.3-S1 -> 9.11.27-S1 and 9.16.8-S1 -> 9.16.11-S1 of BIND Supported Preview Edition. Also release versions 9.17.0 -> 9.17.1 of the BIND 9.17 development branch
CVE-2020-8631	cloud-init through 19.4 relies on Mersenne Twister for a random password, which makes it easier for attackers to predict passwords, because rand_str in cloudinit/util.py calls the random.choice function.
CVE-2020-8632	In cloud-init through 19.4, rand_user_password in cloudinit/config/cc_set_passwords.py has a small default pwlen value, which makes it easier for attackers to guess passwords.
CVE-2020-8648	There is a use-after-free vulnerability in the Linux kernel through 5.5.2 in the n_tty_receive_buf_common function in drivers/tty/n_tty.c.
CVE-2020-8694	Insufficient access control in the Linux kernel driver for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2020-8696	Improper removal of sensitive information before storage or transfer in some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2020-9484	When using Apache Tomcat versions 10.0.0-M1 to 10.0.0-M4, 9.0.0.M1 to 9.0.34, 8.5.0 to 8.5.54 and 7.0.0 to 7.0.103 if a) an attacker is able to control the contents and name of a file on the server; and b) the server is configured to use the PersistenceManager with a FileStore; and c) the PersistenceManager is configured with sessionAttributeValueClassNameFilter="null" (the

	default unless a SecurityManager is used) or a sufficiently lax filter to allow the attacker provided object to be deserialized; and d) the attacker knows the relative file path from the storage location used by FileStore to the file the attacker has control over; then, using a specifically crafted request, the attacker will be able to trigger remote code execution via deserialization of the file under their control. Note that all of conditions a) to d) must be true for the attack to succeed.
CVE-2020-9490	Apache HTTP Server versions 2.4.20 to 2.4.43. A specially crafted value for the 'Cache-Digest' header in a HTTP/2 request would result in a crash when the server actually tries to HTTP/2 PUSH a resource afterwards. Configuring the HTTP/2 feature via "H2Push off" will mitigate this vulnerability for unpatched servers.
CVE-2020-9633	Adobe Flash Player Desktop Runtime 32.0.0.371 and earlier, Adobe Flash Player for Google Chrome 32.0.0.371 and earlier, and Adobe Flash Player for Microsoft Edge and Internet Explorer 32.0.0.330 and earlier have an use after free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2020-9746	Adobe Flash Player version 32.0.0.433 (and earlier) are affected by an exploitable NULL pointer dereference vulnerability that could result in a crash and arbitrary code execution. Exploitation of this issue requires an attacker to insert malicious strings in an HTTP response that is by default delivered over TLS/SSL.
CVE-2021-0127	Insufficient control flow management in some Intel(R) Processors may allow an authenticated user to potentially enable a denial of service via local access.
CVE-2021-0129	Improper access control in BlueZ may allow an authenticated user to potentially enable information disclosure via adjacent access.
CVE-2021-0146	Hardware allows activation of test or debug logic at runtime for some Intel(R) processors which may allow an unauthenticated user to potentially enable escalation of privilege via physical access.
CVE-2021-0326	In p2p_copy_client_info of p2p.c, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution if the target device is performing a Wi-Fi Direct search, with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android-10 Android-11 Android-8.1 Android-9 Android ID: A-172937525
CVE-2021-20178	A flaw was found in ansible module where credentials are disclosed in the console log by default and not protected by the security feature when using the bitbucket_pipeline_variable module. This flaw allows

	an attacker to steal bitbucket_pipeline credentials. The highest threat from this vulnerability is to confidentiality.
CVE-2021-20179	A flaw was found in pki-core. An attacker who has successfully compromised a key could use this flaw to renew the corresponding certificate over and over again, as long as it is not explicitly revoked. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2021-20180	A flaw was found in ansible module where credentials are disclosed in the console log by default and not protected by the security feature when using the bitbucket_pipeline_variable module. This flaw allows an attacker to steal bitbucket_pipeline credentials. The highest threat from this vulnerability is to confidentiality.
CVE-2021-20191	A flaw was found in ansible. Credentials, such as secrets, are being disclosed in console log by default and not protected by no_log feature when using those modules. An attacker can take advantage of this information to steal those credentials. The highest threat from this vulnerability is to data confidentiality. Versions before ansible 2.9.18 are affected.
CVE-2021-20225	A flaw was found in grub2 in versions prior to 2.06. The option parser allows an attacker to write past the end of a heap-allocated buffer by calling certain commands with a large number of specific short forms of options. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-20233	A flaw was found in grub2 in versions prior to 2.06. Setparam_prefix() in the menu rendering code performs a length calculation on the assumption that expressing a quoted single quote will require 3 characters, while it actually requires 4 characters which allows an attacker to corrupt memory by one byte for each quote in the input. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-20254	A flaw was found in samba. The Samba smbd file server must map Windows group identities (SIDs) into unix group ids (gids). The code that performs this had a flaw that could allow it to read data beyond the end of the array in the case where a negative cache entry had been added to the mapping cache. This could cause the calling code to return those values into the process token that stores the group membership for a user. The highest threat from this vulnerability is to data confidentiality and integrity.
CVE-2021-20271	A flaw was found in RPM's signature check functionality when reading a package file. This flaw allows an attacker who can convince a victim to install a seemingly verifiable package, whose signature header

	was modified, to cause RPM database corruption and execute code. The highest threat from this vulnerability is to data integrity, confidentiality, and system availability.
CVE-2021-20277	A flaw was found in Samba's libldb. Multiple, consecutive leading spaces in an LDAP attribute can lead to an out-of-bounds memory write, leading to a crash of the LDAP server process handling the request. The highest threat from this vulnerability is to system availability.
CVE-2021-20294	A flaw was found in binutils readelf 2.35 program. An attacker who is able to convince a victim using readelf to read a crafted file could trigger a stack buffer overflow, out-of-bounds write of arbitrary data supplied by the attacker. The highest impact of this flaw is to confidentiality, integrity, and availability.
CVE-2021-20305	A flaw was found in Nettle in versions before 3.7.2, where several Nettle signature verification functions (GOST DSA, EDDSA & ECDSA) result in the Elliptic Curve Cryptography point (ECC) multiply function being called with out-of-range scalars, possibly resulting in incorrect results. This flaw allows an attacker to force an invalid signature, causing an assertion failure or possible validation. The highest threat to this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2021-20317	A flaw was found in the Linux kernel. A corrupted timer tree caused the task wakeup to be missing in the timerqueue_add function in lib/timerqueue.c. This flaw allows a local attacker with special user privileges to cause a denial of service, slowing and eventually stopping the system while running OSP.
CVE-2021-20321	A race condition accessing file object in the Linux kernel OverlayFS subsystem was found in the way users do rename in specific way with OverlayFS. A local user could use this flaw to crash the system.
CVE-2021-20353	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 194882.
CVE-2021-20492	IBM WebSphere Application Server 8.0, 8.5, 9.0, and Liberty Java Batch is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 197793.
CVE-2021-20579	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5

	could allow a user who can create a view or inline SQL function to obtain sensitive information when AUTO_REVAL is set to DEFERRED_FORCE. IBM X-Force ID: 199283.
CVE-2021-21106	Use after free in autofill in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21107	Use after free in drag and drop in Google Chrome on Linux prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21108	Use after free in media in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21109	Use after free in payments in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21110	Use after free in safe browsing in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21111	Insufficient policy enforcement in WebUI in Google Chrome prior to 87.0.4280.141 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2021-21112	Use after free in Blink in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21113	Heap buffer overflow in Skia in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21114	Use after free in audio in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21115	User after free in safe browsing in Google Chrome prior to 87.0.4280.141 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21116	Heap buffer overflow in audio in Google Chrome prior to 87.0.4280.141 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21117	Insufficient policy enforcement in Cryptohome in Google Chrome prior to 88.0.4324.96 allowed a local attacker

	to perform OS-level privilege escalation via a crafted file.
CVE-2021-21118	Insufficient data validation in V8 in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2021-21119	Use after free in Media in Google Chrome prior to 88.0.4324.96 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21120	Use after free in WebSQL in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21121	Use after free in Omnibox in Google Chrome on Linux prior to 88.0.4324.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21122	Use after free in Blink in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21123	Insufficient data validation in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.
CVE-2021-21124	Potential user after free in Speech Recognizer in Google Chrome on Android prior to 88.0.4324.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21125	Insufficient policy enforcement in File System API in Google Chrome on Windows prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.
CVE-2021-21126	Insufficient policy enforcement in extensions in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass site isolation via a crafted Chrome Extension.
CVE-2021-21127	Insufficient policy enforcement in extensions in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass content security policy via a crafted Chrome Extension.
CVE-2021-21128	Heap buffer overflow in Blink in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21129	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.
CVE-2021-21130	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote

	attacker to bypass filesystem restrictions via a crafted HTML page.
CVE-2021-21131	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.
CVE-2021-21132	Inappropriate implementation in DevTools in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2021-21133	Insufficient policy enforcement in Downloads in Google Chrome prior to 88.0.4324.96 allowed an attacker who convinced a user to download files to bypass navigation restrictions via a crafted HTML page.
CVE-2021-21134	Incorrect security UI in Page Info in Google Chrome on iOS prior to 88.0.4324.96 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2021-21135	Inappropriate implementation in Performance API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-21136	Insufficient policy enforcement in WebView in Google Chrome on Android prior to 88.0.4324.96 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-21137	Inappropriate implementation in DevTools in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to obtain potentially sensitive information from disk via a crafted HTML page.
CVE-2021-21138	Use after free in DevTools in Google Chrome prior to 88.0.4324.96 allowed a local attacker to potentially perform a sandbox escape via a crafted file.
CVE-2021-21139	Inappropriate implementation in iframe sandbox in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2021-21140	Uninitialized use in USB in Google Chrome prior to 88.0.4324.96 allowed a local attacker to potentially perform out of bounds memory access via a USB device.
CVE-2021-21141	Insufficient policy enforcement in File System API in Google Chrome prior to 88.0.4324.96 allowed a remote attacker to bypass file extension policy via a crafted HTML page.
CVE-2021-21142	Use after free in Payments in Google Chrome on Mac prior to 88.0.4324.146 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.

CVE-2021-21143	Heap buffer overflow in Extensions in Google Chrome prior to 88.0.4324.146 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2021-21144	Heap buffer overflow in Tab Groups in Google Chrome prior to 88.0.4324.146 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2021-21145	Use after free in Fonts in Google Chrome prior to 88.0.4324.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21146	Use after free in Navigation in Google Chrome prior to 88.0.4324.146 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21147	Inappropriate implementation in Skia in Google Chrome prior to 88.0.4324.146 allowed a local attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2021-21148	Heap buffer overflow in V8 in Google Chrome prior to 88.0.4324.150 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21149	Stack buffer overflow in Data Transfer in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.
CVE-2021-21150	Use after free in Downloads in Google Chrome on Windows prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21151	Use after free in Payments in Google Chrome prior to 88.0.4324.182 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21152	Heap buffer overflow in Media in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21153	Stack buffer overflow in GPU Process in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2021-21154	Heap buffer overflow in Tab Strip in Google Chrome prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.

CVE-2021-21155	Heap buffer overflow in Tab Strip in Google Chrome on Windows prior to 88.0.4324.182 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21156	Heap buffer overflow in V8 in Google Chrome prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted script.
CVE-2021-21157	Use after free in Web Sockets in Google Chrome on Linux prior to 88.0.4324.182 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21159	Heap buffer overflow in TabStrip in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21160	Heap buffer overflow in WebAudio in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21161	Heap buffer overflow in TabStrip in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21162	Use after free in WebRTC in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21163	Insufficient data validation in Reader Mode in Google Chrome on iOS prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page and a malicious server.
CVE-2021-21165	Data race in audio in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21166	Data race in audio in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21167	Use after free in bookmarks in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21168	Insufficient policy enforcement in appcache in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2021-21169	Out of bounds memory access in V8 in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.

CVE-2021-21170	Incorrect security UI in Loader in Google Chrome prior to 89.0.4389.72 allowed a remote attacker who had compromised the renderer process to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2021-21171	Incorrect security UI in TabStrip and Navigation in Google Chrome on Android prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2021-21172	Insufficient policy enforcement in File System API in Google Chrome on Windows prior to 89.0.4389.72 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page.
CVE-2021-21173	Side-channel information leakage in Network Internals in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-21174	Inappropriate implementation in Referrer in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2021-21175	Inappropriate implementation in Site isolation in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-21176	Inappropriate implementation in full screen mode in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2021-21177	Insufficient policy enforcement in Autofill in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2021-21178	Inappropriate implementation in Compositing in Google Chrome on Linux and Windows prior to 89.0.4389.72 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2021-21179	Use after free in Network Internals in Google Chrome on Linux prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21180	Use after free in tab search in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21181	Side-channel information leakage in autofill in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2021-21182	Insufficient policy enforcement in navigations in Google Chrome prior to 89.0.4389.72 allowed a remote attacker

	who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.
CVE-2021-21183	Inappropriate implementation in performance APIs in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-21184	Inappropriate implementation in performance APIs in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-21185	Insufficient policy enforcement in extensions in Google Chrome prior to 89.0.4389.72 allowed an attacker who convinced a user to install a malicious extension to obtain sensitive information via a crafted Chrome Extension.
CVE-2021-21186	Insufficient policy enforcement in QR scanning in Google Chrome on iOS prior to 89.0.4389.72 allowed an attacker who convinced the user to scan a QR code to bypass navigation restrictions via a crafted QR code.
CVE-2021-21187	Insufficient data validation in URL formatting in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2021-21188	Use after free in Blink in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21189	Insufficient policy enforcement in payments in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2021-21190	Uninitialized data in PDFium in Google Chrome prior to 89.0.4389.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.
CVE-2021-21191	Use after free in WebRTC in Google Chrome prior to 89.0.4389.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21192	Heap buffer overflow in tab groups in Google Chrome prior to 89.0.4389.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21193	Use after free in Blink in Google Chrome prior to 89.0.4389.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21194	Use after free in screen sharing in Google Chrome prior to 89.0.4389.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2021-21195	Use after free in V8 in Google Chrome prior to 89.0.4389.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21196	Heap buffer overflow in TabStrip in Google Chrome on Windows prior to 89.0.4389.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21197	Heap buffer overflow in TabStrip in Google Chrome prior to 89.0.4389.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21198	Out of bounds read in IPC in Google Chrome prior to 89.0.4389.114 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21199	Use after free in Aura in Google Chrome on Linux prior to 89.0.4389.114 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21201	Use after free in permissions in Google Chrome prior to 90.0.4430.72 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21202	Use after free in extensions in Google Chrome prior to 90.0.4430.72 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2021-21203	Use after free in Blink in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21204	Use after free in Blink in Google Chrome on OS X prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21205	Insufficient policy enforcement in navigation in Google Chrome on iOS prior to 90.0.4430.72 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2021-21206	Use after free in Blink in Google Chrome prior to 89.0.4389.128 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21207	Use after free in IndexedDB in Google Chrome prior to 90.0.4430.72 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2021-21208	Insufficient data validation in QR scanner in Google Chrome on iOS prior to 90.0.4430.72 allowed an attacker displaying a QR code to perform domain spoofing via a crafted QR code.

CVE-2021-21209	Inappropriate implementation in storage in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-21210	Inappropriate implementation in Network in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially access local UDP ports via a crafted HTML page.
CVE-2021-21211	Inappropriate implementation in Navigation in Google Chrome on iOS prior to 90.0.4430.72 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-21212	Incorrect security UI in Network Config UI in Google Chrome on ChromeOS prior to 90.0.4430.72 allowed a remote attacker to potentially compromise WiFi connection security via a malicious WAP.
CVE-2021-21213	Use after free in WebMIDI in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21214	Use after free in Network API in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2021-21215	Inappropriate implementation in Autofill in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2021-21216	Inappropriate implementation in Autofill in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to spoof security UI via a crafted HTML page.
CVE-2021-21217	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.
CVE-2021-21218	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.
CVE-2021-21219	Uninitialized data in PDFium in Google Chrome prior to 90.0.4430.72 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted PDF file.
CVE-2021-21220	Insufficient validation of untrusted input in V8 in Google Chrome prior to 89.0.4389.128 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21221	Insufficient validation of untrusted input in Mojo in Google Chrome prior to 90.0.4430.72 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page.

CVE-2021-21222	Heap buffer overflow in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.
CVE-2021-21223	Integer overflow in Mojo in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21224	Type confusion in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2021-21225	Out of bounds memory access in V8 in Google Chrome prior to 90.0.4430.85 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21226	Use after free in navigation in Google Chrome prior to 90.0.4430.85 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-21227	Insufficient data validation in V8 in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21228	Insufficient policy enforcement in extensions in Google Chrome prior to 90.0.4430.93 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.
CVE-2021-21229	Incorrect security UI in downloads in Google Chrome on Android prior to 90.0.4430.93 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2021-21230	Type confusion in V8 in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21231	Insufficient data validation in V8 in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21232	Use after free in Dev Tools in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21233	Heap buffer overflow in ANGLE in Google Chrome on Windows prior to 90.0.4430.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-21261	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. A bug was discovered in the 'flatpak-portal' service that can allow sandboxed applications to execute arbitrary code on the host system (a sandbox escape). This

	<p>sandbox-escape bug is present in versions from 0.11.4 and before fixed versions 1.8.5 and 1.10.0. The Flatpak portal D-Bus service ('flatpak-portal', also known by its D-Bus service name 'org.freedesktop.portal.Flatpak') allows apps in a Flatpak sandbox to launch their own subprocesses in a new sandbox instance, either with the same security settings as the caller or with more restrictive security settings. For example, this is used in Flatpak-packaged web browsers such as Chromium to launch subprocesses that will process untrusted web content, and give those subprocesses a more restrictive sandbox than the browser itself. In vulnerable versions, the Flatpak portal service passes caller-specified environment variables to non-sandboxed processes on the host system, and in particular to the 'flatpak run' command that is used to launch the new sandbox instance. A malicious or compromised Flatpak app could set environment variables that are trusted by the 'flatpak run' command, and use them to execute arbitrary code that is not in a sandbox. As a workaround, this vulnerability can be mitigated by preventing the 'flatpak-portal' service from starting, but that mitigation will prevent many Flatpak apps from working correctly. This is fixed in versions 1.8.5 and 1.10.0.</p>
CVE-2021-21284	In Docker before versions 9.03.15, 20.10.3 there is a vulnerability involving the --userns-remap option in which access to remapped root allows privilege escalation to real root. When using "--userns-remap", if the root user in the remapped namespace has access to the host filesystem they can modify files under "/var/lib/docker/<remapping>" that cause writing files with extended privileges. Versions 20.10.3 and 19.03.15 contain patches that prevent privilege escalation from remapped user.
CVE-2021-21285	In Docker before versions 9.03.15, 20.10.3 there is a vulnerability in which pulling an intentionally malformed Docker image manifest crashes the dockerd daemon. Versions 20.10.3 and 19.03.15 contain patches that prevent the daemon from crashing.
CVE-2021-21300	Git is an open-source distributed revision control system. In affected versions of Git a specially crafted repository that contains symbolic links as well as files using a clean/smudge filter such as Git LFS, may cause just-checked out script to be executed while cloning onto a case-insensitive file system such as NTFS, HFS + or APFS (i.e. the default file systems on Windows and macOS). Note that clean/smudge filters have to be configured for that. Git for Windows configures Git LFS by default, and is therefore vulnerable. The problem has been patched in the versions published on Tuesday, March 9th, 2021. As a workaround, if symbolic link

	<p>support is disabled in Git (e.g. via `git config --global core.symlinks false`), the described attack won't work. Likewise, if no clean/smudge filters such as Git LFS are configured globally (i.e. <code>_before_cloning</code>), the attack is foiled. As always, it is best to avoid cloning repositories from untrusted sources. The earliest impacted version is 2.14.2. The fix versions are: 2.30.1, 2.29.3, 2.28.1, 2.27.1, 2.26.3, 2.25.5, 2.24.4, 2.23.4, 2.22.5, 2.21.4, 2.20.5, 2.19.6, 2.18.5, 2.17.62.17.6.</p>
CVE-2021-21334	<p>In containerd (an industry-standard container runtime) before versions 1.3.10 and 1.4.4, containers launched through containerd's CRI implementation (through Kubernetes, crictl, or any other pod/container client that uses the containerd CRI service) that share the same image may receive incorrect environment variables, including values that are defined for other containers. If the affected containers have different security contexts, this may allow sensitive information to be unintentionally shared. If you are not using containerd's CRI implementation (through one of the mechanisms described above), you are not vulnerable to this issue. If you are not launching multiple containers or Kubernetes pods from the same image which have different environment variables, you are not vulnerable to this issue. If you are not launching multiple containers or Kubernetes pods from the same image in rapid succession, you have reduced likelihood of being vulnerable to this issue. This vulnerability has been fixed in containerd 1.3.10 and containerd 1.4.4. Users should update to these versions.</p>
CVE-2021-21344	<p>XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability which may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.</p>
CVE-2021-21345	<p>XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability which may allow a remote attacker who has sufficient rights to execute commands of the host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.</p>

CVE-2021-21346	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability which may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.
CVE-2021-21347	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability which may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.
CVE-2021-21350	XStream is a Java library to serialize objects to XML and back again. In XStream before version 1.4.16, there is a vulnerability which may allow a remote attacker to execute arbitrary code only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the Security Framework, you will have to use at least version 1.4.16.
CVE-2021-21381	Flatpak is a system for building, distributing, and running sandboxed desktop applications on Linux. In Flatpack since version 0.9.4 and before version 1.10.2 has a vulnerability in the "file forwarding" feature which can be used by an attacker to gain access to files that would not ordinarily be allowed by the app's permissions. By putting the special tokens `@@` and/or `@@@u` in the Exec field of a Flatpak app's .desktop file, a malicious app publisher can trick flatpak into behaving as though the user had chosen to open a target file with their Flatpak app, which automatically makes that file available to the Flatpak app. This is fixed in version 1.10.2. A minimal solution is the first commit "Disallow @@ and @@U usage in desktop files". The follow-up commits "dir: Reserve the whole @@ prefix" and "dir: Refuse to export .desktop files with suspicious uses of @@ tokens" are recommended, but not strictly required. As a workaround, avoid installing Flatpak apps from untrusted sources, or check the contents of the exported `.desktop` files in `exports/`

	share/applications/*.desktop` (typically `~/.local/share/flatpak(exports/share/applications/*.desktop` and `/var/lib/flatpak(exports/share/applications/*.desktop`) to make sure that literal filenames do not follow `@@@` or `@@@u`.
CVE-2021-2144	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Parser). Supported versions that are affected are 5.7.29 and prior and 8.0.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.1 Base Score 7.2 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2021-21602	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier allows reading arbitrary files using the file browser for workspaces and archived artifacts by following symlinks.
CVE-2021-21603	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not escape notification bar response contents, resulting in a cross-site scripting (XSS) vulnerability.
CVE-2021-21604	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier allows attackers with permission to create or configure various objects to inject crafted content into Old Data Monitor that results in the instantiation of potentially unsafe objects once discarded by an administrator.
CVE-2021-21605	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier allows users with Agent/Configure permission to choose agent names that cause Jenkins to override the global `config.xml` file.
CVE-2021-21606	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier improperly validates the format of a provided fingerprint ID when checking for its existence allowing an attacker to check for the existence of XML files with a short path.
CVE-2021-21607	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not limit sizes provided as query parameters to graph-rendering URLs, allowing attackers to request crafted URLs that use all available memory in Jenkins, potentially leading to out of memory errors.
CVE-2021-21608	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not escape button labels in the Jenkins UI, resulting in a cross-site scripting (XSS) vulnerability exploitable by attackers with the ability to control button labels.
CVE-2021-21609	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not correctly match requested URLs to the list of always accessible paths, allowing attackers without Overall/Read permission to access some URLs as if they did have Overall/Read permission.

CVE-2021-2161	Vulnerability in the Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u291, 8u281, 11.0.10, 16; Java SE Embedded: 8u281; Oracle GraalVM Enterprise Edition: 19.3.5, 20.3.1.2 and 21.0.0.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition 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. It can also be exploited by supplying untrusted data to APIs in the specified Component. CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).
CVE-2021-21610	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not implement any restrictions for the URL rendering a formatted preview of markup passed as a query parameter, resulting in a reflected cross-site scripting (XSS) vulnerability if the configured markup formatter does not prohibit unsafe elements (JavaScript) in markup.
CVE-2021-21611	Jenkins 2.274 and earlier, LTS 2.263.1 and earlier does not escape display names and IDs of item types shown on the New Item page, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to specify display names or IDs of item types.
CVE-2021-21615	Jenkins 2.275 and LTS 2.263.2 allows reading arbitrary files using the file browser for workspaces and archived artifacts due to a time-of-check to time-of-use (TOCTOU) race condition.
CVE-2021-2163	Vulnerability in the Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 7u291, 8u281, 11.0.10, 16; Java SE Embedded: 8u281; Oracle GraalVM Enterprise Edition: 19.3.5, 20.3.1.2 and 21.0.0.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java

	SE Embedded, Oracle GraalVM Enterprise Edition 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. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:H/A:N).
CVE-2021-22132	Elasticsearch versions 7.7.0 to 7.10.1 contain an information disclosure flaw in the async search API. Users who execute an async search will improperly store the HTTP headers. An Elasticsearch user with the ability to read the .tasks index could obtain sensitive request headers of other users in the cluster. This issue is fixed in Elasticsearch 7.10.2
CVE-2021-22543	An issue was discovered in Linux: KVM through Improper handling of VM_IO VM_PFNMAP vmas in KVM can bypass RO checks and can lead to pages being freed while still accessible by the VMM and guest. This allows users with the ability to start and control a VM to read/write random pages of memory and can result in local privilege escalation.
CVE-2021-22555	A heap out-of-bounds write affecting Linux since v2.6.19-rc1 was discovered in net/netfilter/x_tables.c. This allows an attacker to gain privileges or cause a DoS (via heap memory corruption) through user name space
CVE-2021-22876	curl 7.1.1 to and including 7.75.0 is vulnerable to an "Exposure of Private Personal Information to an Unauthorized Actor" by leaking credentials in the HTTP Referer: header. libcurl does not strip off user credentials from the URL when automatically populating the Referer: HTTP request header field in outgoing HTTP requests, and therefore risks leaking sensitive data to the server that is the target of the second HTTP request.
CVE-2021-22898	curl 7.7 through 7.76.1 suffers from an information disclosure when the '-t' command line option, known as 'CURLOPT_TELNETOPTIONS' in libcurl, is used to send variable=content pairs to TELNET servers. Due to a flaw in the option parser for sending NEW_ENV variables, libcurl could be made to pass on uninitialized data from a stack based buffer to the server, resulting in potentially revealing sensitive internal information to the server using a clear-text network protocol.
CVE-2021-22922	When curl is instructed to download content using the metalink feature, the contents is verified against a hash provided in the metalink XML file. The metalink XML file points out to the client how to get the same content from a set of different URLs, potentially hosted by different servers and the client can then download the file from one or several of them. In a serial or parallel manner. If

	one of the servers hosting the contents has been breached and the contents of the specific file on that server is replaced with a modified payload, curl should detect this when the hash of the file mismatches after a completed download. It should remove the contents and instead try getting the contents from another URL. This is not done, and instead such a hash mismatch is only mentioned in text and the potentially malicious content is kept in the file on disk.
CVE-2021-22923	When curl is instructed to get content using the metalink feature, and a user name and password are used to download the metalink XML file, those same credentials are then subsequently passed on to each of the servers from which curl will download or try to download the contents from. Often contrary to the user's expectations and intentions and without telling the user it happened.
CVE-2021-22924	libcurl keeps previously used connections in a connection pool for subsequent transfers to reuse, if one of them matches the setup. Due to errors in the logic, the config matching function did not take 'issuercert' into account and it compared the involved paths *case insensitively*, which could lead to libcurl reusing wrong connections. File paths are, or can be, case sensitive on many systems but not all, and can even vary depending on used file systems. The comparison also didn't include the 'issuer cert' which a transfer can set to qualify how to verify the server certificate.
CVE-2021-22925	curl supports the '-t' command line option, known as 'CURLOPT_TELNETOPTIONS' in libcurl. This rarely used option is used to send variable=content pairs to TELNET servers. Due to a flaw in the option parser for sending 'NEW_ENV' variables, libcurl could be made to pass on uninitialized data from a stack-based buffer to the server. Therefore potentially revealing sensitive internal information to the server using a clear-text network protocol. This could happen because curl did not call and use sscanf() correctly when parsing the string provided by the application.
CVE-2021-22945	When sending data to an MQTT server, libcurl <= 7.73.0 and 7.78.0 could in some circumstances erroneously keep a pointer to an already freed memory area and both use that again in a subsequent call to send data and also free it *again*.
CVE-2021-22946	A user can tell curl >= 7.20.0 and <= 7.78.0 to require a successful upgrade to TLS when speaking to an IMAP, POP3 or FTP server ('--ssl-reqd' on the command line or 'CURLOPT_USE_SSL' set to 'CURLUSESSL_CONTROL' or 'CURLUSESSL_ALL' with libcurl). This requirement could be bypassed if the server would return a properly crafted but perfectly legitimate response. This flaw would then make curl

	silently continue its operations **withoutTLS** contrary to the instructions and expectations, exposing possibly sensitive data in clear text over the network.
CVE-2021-22947	When curl >= 7.20.0 and <= 7.78.0 connects to an IMAP or POP3 server to retrieve data using STARTTLS to upgrade to TLS security, the server can respond and send back multiple responses at once that curl caches. curl would then upgrade to TLS but not flush the in-queue of cached responses but instead continue using and trusting the responses it got *before* the TLS handshake as if they were authenticated. Using this flaw, it allows a Man-In-The-Middle attacker to first inject the fake responses, then pass-through the TLS traffic from the legitimate server and trick curl into sending data back to the user thinking the attacker's injected data comes from the TLS-protected server.
CVE-2021-23133	A race condition in Linux kernel SCTP sockets (net/sctp/socket.c) before 5.12-rc8 can lead to kernel privilege escalation from the context of a network service or an unprivileged process. If sctp_destroy_sock is called without sock_net(sk)->sctp.addr_wq_lock then an element is removed from the auto_asconf_splist list without any proper locking. This can be exploited by an attacker with network service privileges to escalate to root or from the context of an unprivileged user directly if a BPF_CGROUP_INET_SOCK_CREATE is attached which denies creation of some SCTP socket.
CVE-2021-23336	The package python/cpython from 0 and before 3.6.13, from 3.7.0 and before 3.7.10, from 3.8.0 and before 3.8.8, from 3.9.0 and before 3.9.2 are vulnerable to Web Cache Poisoning via urllib.parse.parse_qs and urllib.parse.parse_qs by using a vector called parameter cloaking. When the attacker can separate query parameters using a semicolon (;), they can cause a difference in the interpretation of the request between the proxy (running with default configuration) and the server. This can result in malicious requests being cached as completely safe ones, as the proxy would usually not see the semicolon as a separator, and therefore would not include it in a cache key of an unkeyed parameter.
CVE-2021-2341	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Networking). Supported versions that are affected are Java SE: 7u301, 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful

	<p>attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).</p>
CVE-2021-2369	<p>Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Library). Supported versions that are affected are Java SE: 7u301, 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).</p>
CVE-2021-23839	<p>OpenSSL 1.0.2 supports SSLv2. If a client attempts to negotiate SSLv2 with a server that is configured to support both SSLv2 and more recent SSL and TLS versions then a check is made for a version rollback attack when unpadding an RSA signature. Clients that support SSL or TLS versions greater than SSLv2 are supposed to use a special form of padding. A server that supports greater than SSLv2 is supposed to reject connection attempts from a client where this special form of padding is present, because this indicates that a version rollback has occurred (i.e. both client and server support greater than SSLv2, and yet this is the version that is being requested). The implementation of this padding check inverted the logic so that the connection attempt is accepted if the padding is present, and rejected if it is absent. This means that such as server</p>

	<p>will accept a connection if a version rollback attack has occurred. Further the server will erroneously reject a connection if a normal SSLv2 connection attempt is made. Only OpenSSL 1.0.2 servers from version 1.0.2s to 1.0.2x are affected by this issue. In order to be vulnerable a 1.0.2 server must: 1) have configured SSLv2 support at compile time (this is off by default), 2) have configured SSLv2 support at runtime (this is off by default), 3) have configured SSLv2 ciphersuites (these are not in the default ciphersuite list) OpenSSL 1.1.1 does not have SSLv2 support and therefore is not vulnerable to this issue. The underlying error is in the implementation of the RSA_padding_check_SSLv23() function. This also affects the RSA_SSLV23_PADDING padding mode used by various other functions. Although 1.1.1 does not support SSLv2 the RSA_padding_check_SSLv23() function still exists, as does the RSA_SSLV23_PADDING padding mode. Applications that directly call that function or use that padding mode will encounter this issue. However since there is no support for the SSLv2 protocol in 1.1.1 this is considered a bug and not a security issue in that version. OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.0.2y (Affected 1.0.2s-1.0.2x).</p>
CVE-2021-23840	Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissible length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).
CVE-2021-23841	The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref

	<p>and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).</p>
CVE-2021-2388	<p>Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 8u291, 11.0.11, 16.0.1; Oracle GraalVM Enterprise Edition: 20.3.2 and 21.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).</p>
CVE-2021-23953	<p>If a user clicked into a specifically crafted PDF, the PDF reader could be confused into leaking cross-origin information, when said information is served as chunked data. This vulnerability affects Firefox < 85, Thunderbird < 78.7, and Firefox ESR < 78.7.</p>
CVE-2021-23954	<p>Using the new logical assignment operators in a JavaScript switch statement could have caused a type confusion, leading to a memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 85, Thunderbird < 78.7, and Firefox ESR < 78.7.</p>
CVE-2021-23960	<p>Performing garbage collection on re-declared JavaScript variables resulted in a user-after-poison, and a potentially exploitable crash. This vulnerability affects</p>

	Firefox < 85, Thunderbird < 78.7, and Firefox ESR < 78.7.
CVE-2021-23961	Further techniques that built on the slipstream research combined with a malicious webpage could have exposed both an internal network's hosts as well as services running on the user's local machine. This vulnerability affects Firefox < 85.
CVE-2021-23964	Mozilla developers reported memory safety bugs present in Firefox 84 and Firefox ESR 78.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 85, Thunderbird < 78.7, and Firefox ESR < 78.7.
CVE-2021-23968	If Content Security Policy blocked frame navigation, the full destination of a redirect served in the frame was reported in the violation report; as opposed to the original frame URI. This could be used to leak sensitive information contained in such URLs. This vulnerability affects Firefox < 86, Thunderbird < 78.8, and Firefox ESR < 78.8.
CVE-2021-23969	As specified in the W3C Content Security Policy draft, when creating a violation report, "User agents need to ensure that the source file is the URL requested by the page, pre-redirects. If that's not possible, user agents need to strip the URL down to an origin to avoid unintentional leakage." Under certain types of redirects, Firefox incorrectly set the source file to be the destination of the redirects. This was fixed to be the redirect destination's origin. This vulnerability affects Firefox < 86, Thunderbird < 78.8, and Firefox ESR < 78.8.
CVE-2021-23973	When trying to load a cross-origin resource in an audio/video context a decoding error may have resulted, and the content of that error may have revealed information about the resource. This vulnerability affects Firefox < 86, Thunderbird < 78.8, and Firefox ESR < 78.8.
CVE-2021-23978	Mozilla developers reported memory safety bugs present in Firefox 85 and Firefox ESR 78.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 86, Thunderbird < 78.8, and Firefox ESR < 78.8.
CVE-2021-23981	A texture upload of a Pixel Buffer Object could have confused the WebGL code to skip binding the buffer used to unpack it, resulting in memory corruption and a potentially exploitable information leak or crash. This vulnerability affects Firefox ESR < 78.9, Firefox < 87, and Thunderbird < 78.9.

CVE-2021-23982	Using techniques that built on the slipstream research, a malicious webpage could have scanned both an internal network's hosts as well as services running on the user's local machine utilizing WebRTC connections. This vulnerability affects Firefox ESR < 78.9, Firefox < 87, and Thunderbird < 78.9.
CVE-2021-23984	A malicious extension could have opened a popup window lacking an address bar. The title of the popup lacking an address bar should not be fully controllable, but in this situation was. This could have been used to spoof a website and attempt to trick the user into providing credentials. This vulnerability affects Firefox ESR < 78.9, Firefox < 87, and Thunderbird < 78.9.
CVE-2021-23987	Mozilla developers and community members reported memory safety bugs present in Firefox 86 and Firefox ESR 78.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 78.9, Firefox < 87, and Thunderbird < 78.9.
CVE-2021-23991	If a Thunderbird user has previously imported Alice's OpenPGP key, and Alice has extended the validity period of her key, but Alice's updated key has not yet been imported, an attacker may send an email containing a crafted version of Alice's key with an invalid subkey, Thunderbird might subsequently attempt to use the invalid subkey, and will fail to send encrypted email to Alice. This vulnerability affects Thunderbird < 78.9.1.
CVE-2021-23992	Thunderbird did not check if the user ID associated with an OpenPGP key has a valid self signature. An attacker may create a crafted version of an OpenPGP key, by either replacing the original user ID, or by adding another user ID. If Thunderbird imports and accepts the crafted key, the Thunderbird user may falsely conclude that the false user ID belongs to the correspondent. This vulnerability affects Thunderbird < 78.9.1.
CVE-2021-23993	An attacker may perform a DoS attack to prevent a user from sending encrypted email to a correspondent. If an attacker creates a crafted OpenPGP key with a subkey that has an invalid self signature, and the Thunderbird user imports the crafted key, then Thunderbird may try to use the invalid subkey, but the RNP library rejects it from being used, causing encryption to fail. This vulnerability affects Thunderbird < 78.9.1.
CVE-2021-23994	A WebGL framebuffer was not initialized early enough, resulting in memory corruption and an out of bound write. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88.

CVE-2021-23995	When Responsive Design Mode was enabled, it used references to objects that were previously freed. We presume that with enough effort this could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88.
CVE-2021-23998	Through complicated navigations with new windows, an HTTP page could have inherited a secure lock icon from an HTTPS page. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88.
CVE-2021-23999	If a Blob URL was loaded through some unusual user interaction, it could have been loaded by the System Principal and granted additional privileges that should not be granted to web content. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88.
CVE-2021-24002	When a user clicked on an FTP URL containing encoded newline characters (%0A and %0D), the newlines would have been interpreted as such and allowed arbitrary commands to be sent to the FTP server. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88.
CVE-2021-24307	The All in One SEO – Best WordPress SEO Plugin – Easily Improve Your SEO Rankings before 4.1.0.2 enables authenticated users with "aioseo_tools_settings" privilege (most of the time admin) to execute arbitrary code on the underlying host. Users can restore plugin's configuration by uploading a backup .ini file in the section "Tool > Import/Export". However, the plugin attempts to unserialize values of the .ini file. Moreover, the plugin embeds Monolog library which can be used to craft a gadget chain and thus trigger system command execution.
CVE-2021-2432	Vulnerability in the Java SE product of Oracle Java SE (component: JNDI). The supported version that is affected is Java SE: 7u301. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, 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 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).

CVE-2021-24620	The WordPress Simple Ecommerce Shopping Cart Plugin- Sell products through Paypal plugin through 2.2.5 does not check for the uploaded Downloadable Digital product file, allowing any file, such as PHP to be uploaded by an administrator. Furthermore, as there is no CSRF in place, attackers could also make a logged admin upload a malicious PHP file, which would lead to RCE
CVE-2021-25214	In BIND 9.8.5 -> 9.8.8, 9.9.3 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.9.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND 9 Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.11 of the BIND 9.17 development branch, when a vulnerable version of named receives a malformed IXFR triggering the flaw described above, the named process will terminate due to a failed assertion the next time the transferred secondary zone is refreshed.
CVE-2021-25215	In BIND 9.0.0 -> 9.11.29, 9.12.0 -> 9.16.13, and versions BIND 9.9.3-S1 -> 9.11.29-S1 and 9.16.8-S1 -> 9.16.13-S1 of BIND Supported Preview Edition, as well as release versions 9.17.0 -> 9.17.11 of the BIND 9.17 development branch, when a vulnerable version of named receives a query for a record triggering the flaw described above, the named process will terminate due to a failed assertion check. The vulnerability affects all currently maintained BIND 9 branches (9.11, 9.11-S, 9.16, 9.16-S, 9.17) as well as all other versions of BIND 9.
CVE-2021-25217	In ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16, ISC DHCP 4.4.0 -> 4.4.2 (Other branches of ISC DHCP (i.e., releases in the 4.0.x series or lower and releases in the 4.3.x series) are beyond their End-of-Life (EOL) and no longer supported by ISC. From inspection it is clear that the defect is also present in releases from those series, but they have not been officially tested for the vulnerability), The outcome of encountering the defect while reading a lease that will trigger it varies, according to: the component being affected (i.e., dhclient or dhcpcd) whether the package was built as a 32-bit or 64-bit binary whether the compiler flag -fstack-protection-strong was used when compiling In dhclient, ISC has not successfully reproduced the error on a 64-bit system. However, on a 32-bit system it is possible to cause dhclient to crash when reading an improper lease, which could cause network connectivity problems for an affected system due to the absence of a running DHCP client process. In dhcpcd, when run in DHCPv4 or DHCPv6 mode: if the dhcpcd server binary was built for a 32-bit architecture AND the -fstack-protection-strong flag was specified to the compiler, dhcpcd may exit while parsing a lease file containing an objectionable lease, resulting in lack of service to clients. Additionally, the

	offending lease and the lease immediately following it in the lease database may be improperly deleted. if the dhcpcd server binary was built for a 64-bit architecture OR if the -fstack-protection-strong compiler flag was NOT specified, the crash will not occur, but it is possible for the offending lease and the lease which immediately followed it to be improperly deleted.
CVE-2021-26072	The WidgetConnector plugin in Confluence Server and Confluence Data Center before version 5.8.6 allowed remote attackers to manipulate the content of internal network resources via a blind Server-Side Request Forgery (SSRF) vulnerability.
CVE-2021-26084	In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. The affected versions are before version 6.13.23, from version 6.14.0 before 7.4.11, from version 7.5.0 before 7.11.6, and from version 7.12.0 before 7.12.5.
CVE-2021-26085	Affected versions of Atlassian Confluence Server allow remote attackers to view restricted resources via a Pre-Authorization Arbitrary File Read vulnerability in the /s/ endpoint. The affected versions are before version 7.4.10, and from version 7.5.0 before 7.12.3.
CVE-2021-26341	Some AMD CPUs may transiently execute beyond unconditional direct branches, which may potentially result in data leakage.
CVE-2021-26401	LFENCE/JMP (mitigation V2-2) may not sufficiently mitigate CVE-2017-5715 on some AMD CPUs.
CVE-2021-26690	Apache HTTP Server versions 2.4.0 to 2.4.46 A specially crafted Cookie header handled by mod_session can cause a NULL pointer dereference and crash, leading to a possible Denial Of Service
CVE-2021-26691	In Apache HTTP Server versions 2.4.0 to 2.4.46 a specially crafted SessionHeader sent by an origin server could cause a heap overflow
CVE-2021-26814	Wazuh API in Wazuh from 4.0.0 to 4.0.3 allows authenticated users to execute arbitrary code with administrative privileges via /manager/files URI. An authenticated user to the service may exploit incomplete input validation on the /manager/files API to inject arbitrary code within the API service script.
CVE-2021-26930	An issue was discovered in the Linux kernel 3.11 through 5.10.16, as used by Xen. To service requests to the PV backend, the driver maps grant references provided by the frontend. In this process, errors may be encountered. In one case, an error encountered earlier might be discarded by later processing, resulting in the caller assuming successful mapping, and hence

	subsequent operations trying to access space that wasn't mapped. In another case, internal state would be insufficiently updated, preventing safe recovery from the error. This affects drivers/block/xen-blkback/blkback.c.
CVE-2021-26931	An issue was discovered in the Linux kernel 2.6.39 through 5.10.16, as used in Xen. Block, net, and SCSI backends consider certain errors a plain bug, deliberately causing a kernel crash. For errors potentially being at least under the influence of guests (such as out of memory conditions), it isn't correct to assume a plain bug. Memory allocations potentially causing such crashes occur only when Linux is running in PV mode, though. This affects drivers/block/xen-blkback/blkback.c and drivers/xen/xen-scsiback.c.
CVE-2021-26932	An issue was discovered in the Linux kernel 3.2 through 5.10.16, as used by Xen. Grant mapping operations often occur in batch hypercalls, where a number of operations are done in a single hypercall, the success or failure of each one is reported to the backend driver, and the backend driver then loops over the results, performing follow-up actions based on the success or failure of each operation. Unfortunately, when running in PV mode, the Linux backend drivers mishandle this: Some errors are ignored, effectively implying their success from the success of related batch elements. In other cases, errors resulting from one batch element lead to further batch elements not being inspected, and hence successful ones to not be possible to properly unmap upon error recovery. Only systems with Linux backends running in PV mode are vulnerable. Linux backends run in HVM / PVH modes are not vulnerable. This affects arch/*/xen/p2m.c and drivers/xen/gntdev.c.
CVE-2021-26937	encoding.c in GNU Screen through 4.8.0 allows remote attackers to cause a denial of service (invalid write access and application crash) or possibly have unspecified other impact via a crafted UTF-8 character sequence.
CVE-2021-27135	xterm before Patch #366 allows remote attackers to execute arbitrary code or cause a denial of service (segmentation fault) via a crafted UTF-8 combining character sequence.
CVE-2021-27218	An issue was discovered in GNOME GLib before 2.66.7 and 2.67.x before 2.67.4. If g_byte_array_new_take() was called with a buffer of 4GB or more on a 64-bit platform, the length would be truncated modulo 2^{32} , causing unintended length truncation.
CVE-2021-27219	An issue was discovered in GNOME GLib before 2.66.6 and 2.67.x before 2.67.3. The function g_bytes_new has an integer overflow on 64-bit platforms due to an implicit cast from 64 bits to 32 bits. The overflow could potentially lead to memory corruption.

CVE-2021-27363	An issue was discovered in the Linux kernel through 5.11.3. A kernel pointer leak can be used to determine the address of the <code>iscsi_transport</code> structure. When an iSCSI transport is registered with the iSCSI subsystem, the transport's handle is available to unprivileged users via the sysfs file system, at <code>/sys/class/iscsi_transport/\$TRANSPORT_NAME/handle</code> . When read, the <code>show_transport_handle</code> function (in <code>drivers/scsi/scsi_transport_iscsi.c</code>) is called, which leaks the handle. This handle is actually the pointer to an <code>iscsi_transport</code> struct in the kernel module's global variables.
CVE-2021-27364	An issue was discovered in the Linux kernel through 5.11.3. <code>drivers/scsi/scsi_transport_iscsi.c</code> is adversely affected by the ability of an unprivileged user to craft Netlink messages.
CVE-2021-27365	An issue was discovered in the Linux kernel through 5.11.3. Certain iSCSI data structures do not have appropriate length constraints or checks, and can exceed the <code>PAGE_SIZE</code> value. An unprivileged user can send a Netlink message that is associated with iSCSI, and has a length up to the maximum length of a Netlink message.
CVE-2021-27803	A vulnerability was discovered in how <code>p2p/p2p_pd.c</code> in <code>wpa_supplicant</code> before 2.10 processes P2P (Wi-Fi Direct) provision discovery requests. It could result in denial of service or other impact (potentially execution of arbitrary code), for an attacker within radio range.
CVE-2021-27918	<code>encoding/xml</code> in Go before 1.15.9 and 1.16.x before 1.16.1 has an infinite loop if a custom <code>TokenReader</code> (for <code>xml.NewTokenDecoder</code>) returns EOF in the middle of an element. This can occur in the <code>Decode</code> , <code>DecodeElement</code> , or <code>Skip</code> method.
CVE-2021-27919	<code>archive/zip</code> in Go 1.16.x before 1.16.1 allows attackers to cause a denial of service (panic) upon attempted use of the <code>Reader.Open</code> API for a ZIP archive in which <code>..</code> occurs at the beginning of any filename.
CVE-2021-28038	An issue was discovered in the Linux kernel through 5.11.3, as used with Xen PV. A certain part of the netback driver lacks necessary treatment of errors such as failed memory allocations (as a result of changes to the handling of grant mapping errors). A host OS denial of service may occur during misbehavior of a networking frontend driver. NOTE: this issue exists because of an incomplete fix for CVE-2021-26931.
CVE-2021-28091	Lasso all versions prior to 2.7.0 has improper verification of a cryptographic signature.
CVE-2021-28133	Zoom through 5.5.4 sometimes allows attackers to read private information on a participant's screen, even though the participant never attempted to share the private part of their screen. When a user shares

	a specific application window via the Share Screen functionality, other meeting participants can briefly see contents of other application windows that were explicitly not shared. The contents of these other windows can (for instance) be seen for a short period of time when they overlay the shared window and get into focus. (An attacker can, of course, use a separate screen-recorder application, unsupported by Zoom, to save all such contents for later replays and analysis.) Depending on the unintentionally shared data, this short exposure of screen contents may be a more or less severe security issue.
CVE-2021-28363	The urllib3 library 1.26.x before 1.26.4 for Python omits SSL certificate validation in some cases involving HTTPS to HTTPS proxies. The initial connection to the HTTPS proxy (if an SSLContext isn't given via proxy_config) doesn't verify the hostname of the certificate. This means certificates for different servers that still validate properly with the default urllib3 SSLContext will be silently accepted.
CVE-2021-28375	An issue was discovered in the Linux kernel through 5.11.6. fastrpc_internal_invoke in drivers/misc/fastrpc.c does not prevent user applications from sending kernel RPC messages, aka CID-20c40794eb85. This is a related issue to CVE-2019-2308.
CVE-2021-28660	rtw_wx_set_scan in drivers/staging/rtl8188eu/os_dep/ioctl_linux.c in the Linux kernel through 5.11.6 allows writing beyond the end of the ->ssid[] array. NOTE: from the perspective of kernel.org releases, CVE IDs are not normally used for drivers/staging/* (unfinished work); however, system integrators may have situations in which a drivers/staging issue is relevant to their own customer base.
CVE-2021-28688	The fix for XSA-365 includes initialization of pointers such that subsequent cleanup code wouldn't use uninitialized or stale values. This initialization went too far and may under certain conditions also overwrite pointers which are in need of cleaning up. The lack of cleanup would result in leaking persistent grants. The leak in turn would prevent fully cleaning up after a respective guest has died, leaving around zombie domains. All Linux versions having the fix for XSA-365 applied are vulnerable. XSA-365 was classified to affect versions back to at least 3.11.
CVE-2021-28691	Guest triggered use-after-free in Linux xen-netback A malicious or buggy network PV frontend can force Linux netback to disable the interface and terminate the receive kernel thread associated with queue 0 in response to the frontend sending a malformed packet. Such kernel thread termination will lead to a use-after-free in Linux netback when the backend is destroyed,

	as the kernel thread associated with queue 0 will have already exited and thus the call to kthread_stop will be performed against a stale pointer.
CVE-2021-28711	Rogue backends can cause DoS of guests via high frequency events T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Xen offers the ability to run PV backends in regular unprivileged guests, typically referred to as "driver domains". Running PV backends in driver domains has one primary security advantage: if a driver domain gets compromised, it doesn't have the privileges to take over the system. However, a malicious driver domain could try to attack other guests via sending events at a high frequency leading to a Denial of Service in the guest due to trying to service interrupts for elongated amounts of time. There are three affected backends: * blkfront patch 1, CVE-2021-28711 * netfront patch 2, CVE-2021-28712 * hvc_xen (console) patch 3, CVE-2021-28713
CVE-2021-28712	Rogue backends can cause DoS of guests via high frequency events T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Xen offers the ability to run PV backends in regular unprivileged guests, typically referred to as "driver domains". Running PV backends in driver domains has one primary security advantage: if a driver domain gets compromised, it doesn't have the privileges to take over the system. However, a malicious driver domain could try to attack other guests via sending events at a high frequency leading to a Denial of Service in the guest due to trying to service interrupts for elongated amounts of time. There are three affected backends: * blkfront patch 1, CVE-2021-28711 * netfront patch 2, CVE-2021-28712 * hvc_xen (console) patch 3, CVE-2021-28713
CVE-2021-28713	Rogue backends can cause DoS of guests via high frequency events T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Xen offers the ability to run PV backends in regular unprivileged guests, typically referred to as "driver domains". Running PV backends in driver domains has one primary security advantage: if a driver domain gets compromised, it doesn't have the privileges to take over the system. However, a malicious driver domain could try to attack other guests via sending events at a high frequency leading to a Denial of Service in the guest due to trying to service interrupts for elongated amounts of time. There are three affected backends: * blkfront patch 1, CVE-2021-28711 * netfront patch

	2, CVE-2021-28712 * hvc_xen (console) patch 3, CVE-2021-28713
CVE-2021-28714	Guest can force Linux netback driver to hog large amounts of kernel memory [his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Incoming data packets for a guest in the Linux kernel's netback driver are buffered until the guest is ready to process them. There are some measures taken for avoiding to pile up too much data, but those can be bypassed by the guest: There is a timeout how long the client side of an interface can stop consuming new packets before it is assumed to have stalled, but this timeout is rather long (60 seconds by default). Using a UDP connection on a fast interface can easily accumulate gigabytes of data in that time. (CVE-2021-28715) The timeout could even never trigger if the guest manages to have only one free slot in its RX queue ring page and the next package would require more than one free slot, which may be the case when using GSO, XDP, or software hashing. (CVE-2021-28714)
CVE-2021-28715	Guest can force Linux netback driver to hog large amounts of kernel memory [his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Incoming data packets for a guest in the Linux kernel's netback driver are buffered until the guest is ready to process them. There are some measures taken for avoiding to pile up too much data, but those can be bypassed by the guest: There is a timeout how long the client side of an interface can stop consuming new packets before it is assumed to have stalled, but this timeout is rather long (60 seconds by default). Using a UDP connection on a fast interface can easily accumulate gigabytes of data in that time. (CVE-2021-28715) The timeout could even never trigger if the guest manages to have only one free slot in its RX queue ring page and the next package would require more than one free slot, which may be the case when using GSO, XDP, or software hashing. (CVE-2021-28714)
CVE-2021-28876	In the standard library in Rust before 1.52.0, the Zip implementation has a panic safety issue. It calls <code>__iterator_get_unchecked()</code> more than once for the same index when the underlying iterator panics (in certain conditions). This bug could lead to a memory safety violation due to an unmet safety requirement for the <code>TrustedRandomAccess</code> trait.
CVE-2021-28878	In the standard library in Rust before 1.52.0, the Zip implementation calls <code>__iterator_get_unchecked()</code> more than once for the same index (under certain

	conditions) when next_back() and next() are used together. This bug could lead to a memory safety violation due to an unmet safety requirement for the TrustedRandomAccess trait.
CVE-2021-28879	In the standard library in Rust before 1.52.0, the Zip implementation can report an incorrect size due to an integer overflow. This bug can lead to a buffer overflow when a consumed Zip iterator is used again.
CVE-2021-28964	A race condition was discovered in get_old_root in fs/btrfs/ctree.c in the Linux kernel through 5.11.8. It allows attackers to cause a denial of service (BUG) because of a lack of locking on an extent buffer before a cloning operation, aka CID-dbcc7d57bffc.
CVE-2021-28971	In intel_pmu_drain_pebs_nhm in arch/x86/events/intel/ds.c in the Linux kernel through 5.11.8 on some Haswell CPUs, userspace applications (such as perf-fuzzer) can cause a system crash because the PEBS status in a PEBS record is mishandled, aka CID-d88d05a9e0b6.
CVE-2021-28972	In drivers/pci/hotplug/rpadlpar_sysfs.c in the Linux kernel through 5.11.8, the RPA PCI Hotplug driver has a user-tolerable buffer overflow when writing a new device name to the driver from userspace, allowing userspace to write data to the kernel stack frame directly. This occurs because add_slot_store and remove_slot_store mishandle drc_name '\0' termination, aka CID-cc7a0bb058b8.
CVE-2021-29154	BPF JIT compilers in the Linux kernel through 5.11.12 have incorrect computation of branch displacements, allowing them to execute arbitrary code within the kernel context. This affects arch/x86/net/bpf_jit_comp.c and arch/x86/net/bpf_jit_comp32.c.
CVE-2021-29155	An issue was discovered in the Linux kernel through 5.11.x. kernel/bpf/verifier.c performs undesirable out-of-bounds speculation on pointer arithmetic, leading to side-channel attacks that defeat Spectre mitigations and obtain sensitive information from kernel memory. Specifically, for sequences of pointer arithmetic operations, the pointer modification performed by the first operation is not correctly accounted for when restricting subsequent operations.
CVE-2021-29265	An issue was discovered in the Linux kernel before 5.11.7. usblip_sockfd_store in drivers/usb/usblip/stub_dev.c allows attackers to cause a denial of service (GPF) because the stub-up sequence has race conditions during an update of the local and shared status, aka CID-9380afdf70.
CVE-2021-29338	Integer Overflow in OpenJPEG v2.4.0 allows remote attackers to crash the application, causing a Denial of Service (DoS). This occurs when the attacker uses

	the command line option "-ImgDir" on a directory that contains 1048576 files.
CVE-2021-29457	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A heap buffer overflow was found in Exiv2 versions v0.27.3 and earlier. The heap overflow is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to gain code execution, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when _writing_ the metadata, which is a less frequently used Exiv2 operation than _reading_ the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as `insert`. The bug is fixed in version v0.27.4.
CVE-2021-29505	XStream is software for serializing Java objects to XML and back again. A vulnerability in XStream versions prior to 1.4.17 may allow a remote attacker has sufficient rights to execute commands of the host only by manipulating the processed input stream. No user who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types is affected. The vulnerability is patched in version 1.4.17.
CVE-2021-29647	An issue was discovered in the Linux kernel before 5.11.11. qrtr_recvmsg in net/qrtr/qrtr.c allows attackers to obtain sensitive information from kernel memory because of a partially uninitialized data structure, aka CID-50535249f624.
CVE-2021-29650	An issue was discovered in the Linux kernel before 5.11.11. The netfilter subsystem allows attackers to cause a denial of service (panic) because net/netfilter/x_tables.c and include/linux/netfilter/x_tables.h lack a full memory barrier upon the assignment of a new table value, aka CID-175e476b8cdf.
CVE-2021-29702	Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1.4 and 11.5.5 is vulnerable to a denial of service as the server terminates abnormally when executing a specially crafted SELECT statement. IBM X-Force ID: 200658.
CVE-2021-29703	Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to a denial of service as the server terminates abnormally when executing a specially crafted SELECT statement. IBM X-Force ID: 200659.
CVE-2021-29777	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5, under specific circumstance of a table being dropped while being accessed in another session, could allow an

	authenticated user to cause a denial of service IBM X-Force ID: 203031.
CVE-2021-29945	The WebAssembly JIT could miscalculate the size of a return type, which could lead to a null read and result in a crash. *Note: This issue only affected x86-32 platforms. Other platforms are unaffected.*. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88.
CVE-2021-29946	Ports that were written as an integer overflow above the bounds of a 16-bit integer could have bypassed port blocking restrictions when used in the Alt-Svc header. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88.
CVE-2021-29948	Signatures are written to disk before and read during verification, which might be subject to a race condition when a malicious local process or user is replacing the file. This vulnerability affects Thunderbird < 78.10.
CVE-2021-29956	OpenPGP secret keys that were imported using Thunderbird version 78.8.1 up to version 78.10.1 were stored unencrypted on the user's local disk. The master password protection was inactive for those keys. Version 78.10.2 will restore the protection mechanism for newly imported keys, and will automatically protect keys that had been imported using affected Thunderbird versions. This vulnerability affects Thunderbird < 78.10.2.
CVE-2021-29957	If a MIME encoded email contains an OpenPGP inline signed or encrypted message part, but also contains an additional unprotected part, Thunderbird did not indicate that only parts of the message are protected. This vulnerability affects Thunderbird < 78.10.2.
CVE-2021-29967	Mozilla developers reported memory safety bugs present in Firefox 88 and Firefox ESR 78.11. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 78.11, Firefox < 89, and Firefox ESR < 78.11.
CVE-2021-29969	If Thunderbird was configured to use STARTTLS for an IMAP connection, and an attacker injected IMAP server responses prior to the completion of the STARTTLS handshake, then Thunderbird didn't ignore the injected data. This could have resulted in Thunderbird showing incorrect information, for example the attacker could have tricked Thunderbird to show folders that didn't exist on the IMAP server. This vulnerability affects Thunderbird < 78.12.
CVE-2021-29970	A malicious webpage could have triggered a use-after-free, memory corruption, and a potentially exploitable crash. *This bug could only be triggered

	when accessibility was enabled.*. This vulnerability affects Thunderbird < 78.12, Firefox ESR < 78.12, and Firefox < 90.
CVE-2021-29976	Mozilla developers reported memory safety bugs present in code shared between Firefox and Thunderbird. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 78.12, Firefox ESR < 78.12, and Firefox < 90.
CVE-2021-29980	Uninitialized memory in a canvas object could have caused an incorrect free() leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.
CVE-2021-29984	Instruction reordering resulted in a sequence of instructions that would cause an object to be incorrectly considered during garbage collection. This led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.
CVE-2021-29985	A use-after-free vulnerability in media channels could have led to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.
CVE-2021-29986	A suspected race condition when calling getaddrinfo led to memory corruption and a potentially exploitable crash. *Note: This issue only affected Linux operating systems. Other operating systems are unaffected.* This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.
CVE-2021-29988	Firefox incorrectly treated an inline list-item element as a block element, resulting in an out of bounds read or memory corruption, and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.13, Thunderbird < 91, Firefox ESR < 78.13, and Firefox < 91.
CVE-2021-29989	Mozilla developers reported memory safety bugs present in Firefox 90 and Firefox ESR 78.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 78.13, Firefox ESR < 78.13, and Firefox < 91.
CVE-2021-30465	runc before 1.0.0-rc95 allows a Container Filesystem Breakout via Directory Traversal. To exploit the vulnerability, an attacker must be able to create multiple containers with a fairly specific mount configuration.

	The problem occurs via a symlink-exchange attack that relies on a race condition.
CVE-2021-30506	Incorrect security UI in Web App Installs in Google Chrome on Android prior to 90.0.4430.212 allowed an attacker who convinced a user to install a web application to inject scripts or HTML into a privileged page via a crafted HTML page.
CVE-2021-30507	Inappropriate implementation in Offline in Google Chrome on Android prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.
CVE-2021-30508	Heap buffer overflow in Media Feeds in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to enable certain features in Chrome to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30509	Out of bounds write in Tab Strip in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page and a crafted Chrome extension.
CVE-2021-30510	Use after free in Aura in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30511	Out of bounds read in Tab Groups in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted HTML page.
CVE-2021-30512	Use after free in Notifications in Google Chrome prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30513	Type confusion in V8 in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30514	Use after free in Autofill in Google Chrome prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30515	Use after free in File API in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30516	Heap buffer overflow in History in Google Chrome prior to 90.0.4430.212 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.

CVE-2021-30517	Type confusion in V8 in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30518	Heap buffer overflow in Reader Mode in Google Chrome prior to 90.0.4430.212 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30519	Use after free in Payments in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious payments app to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30520	Use after free in Tab Strip in Google Chrome prior to 90.0.4430.212 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30521	Heap buffer overflow in Autofill in Google Chrome on Android prior to 91.0.4472.77 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.
CVE-2021-30522	Use after free in WebAudio in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30523	Use after free in WebRTC in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit heap corruption via a crafted SCTP packet.
CVE-2021-30524	Use after free in TabStrip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30525	Use after free in TabGroups in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30526	Out of bounds write in TabStrip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page.
CVE-2021-30527	Use after free in WebUI in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30528	Use after free in WebAuthentication in Google Chrome on Android prior to 91.0.4472.77 allowed a remote attacker who had compromised the renderer process of a user who had saved a credit card in their Google account to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30529	Use after free in Bookmarks in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a

	user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30530	Out of bounds memory access in WebAudio in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.
CVE-2021-30531	Insufficient policy enforcement in Content Security Policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2021-30532	Insufficient policy enforcement in Content Security Policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2021-30533	Insufficient policy enforcement in PopupBlocker in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass navigation restrictions via a crafted iframe.
CVE-2021-30534	Insufficient policy enforcement in iFrameSandbox in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2021-30535	Double free in ICU in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30536	Out of bounds read in V8 in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page.
CVE-2021-30537	Insufficient policy enforcement in cookies in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass cookie policy via a crafted HTML page.
CVE-2021-30538	Insufficient policy enforcement in content security policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2021-30539	Insufficient policy enforcement in content security policy in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2021-30540	Incorrect security UI in payments in Google Chrome on Android prior to 91.0.4472.77 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2021-30541	Use after free in V8 in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30542	Use after free in Tab Strip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user

	to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30543	Use after free in Tab Strip in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30544	Use after free in BFCache in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30545	Use after free in Extensions in Google Chrome prior to 91.0.4472.101 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30546	Use after free in Autofill in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30547	Out of bounds write in ANGLE in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2021-30548	Use after free in Loader in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30549	Use after free in Spell check in Google Chrome prior to 91.0.4472.101 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30550	Use after free in Accessibility in Google Chrome prior to 91.0.4472.101 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30551	Type confusion in V8 in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30552	Use after free in Extensions in Google Chrome prior to 91.0.4472.101 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30553	Use after free in Network service in Google Chrome prior to 91.0.4472.101 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30554	Use after free in WebGL in Google Chrome prior to 91.0.4472.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30555	Use after free in Sharing in Google Chrome prior to 91.0.4472.114 allowed an attacker who convinced a user to install a malicious extension to potentially exploit

	heap corruption via a crafted HTML page and user gesture.
CVE-2021-30556	Use after free in WebAudio in Google Chrome prior to 91.0.4472.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30557	Use after free in TabGroups in Google Chrome prior to 91.0.4472.114 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30559	Out of bounds write in ANGLE in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30560	Use after free in Blink XSLT in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30561	Type Confusion in V8 in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30562	Use after free in WebSerial in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30563	Type Confusion in V8 in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30564	Heap buffer overflow in WebXR in Google Chrome prior to 91.0.4472.164 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30565	Out of bounds write in Tab Groups in Google Chrome on Linux and ChromeOS prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page.
CVE-2021-30566	Stack buffer overflow in Printing in Google Chrome prior to 92.0.4515.107 allowed a remote attacker who had compromised the renderer process to potentially exploit stack corruption via a crafted HTML page.
CVE-2021-30567	Use after free in DevTools in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to open DevTools to potentially exploit heap corruption via specific user gesture.
CVE-2021-30568	Heap buffer overflow in WebGL in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2021-30569	Use after free in sqlite in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30571	Insufficient policy enforcement in DevTools in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-30572	Use after free in Autocomplete in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30573	Use after free in GPU in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30574	Use after free in protocol handling in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30575	Out of bounds write in Autocomplete in Google Chrome prior to 92.0.4515.107 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30576	Use after free in DevTools in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30578	Uninitialized use in Media in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to perform out of bounds memory access via a crafted HTML page.
CVE-2021-30579	Use after free in UI framework in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30581	Use after free in DevTools in Google Chrome prior to 92.0.4515.107 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30582	Inappropriate implementation in Animation in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-30584	Incorrect security UI in Downloads in Google Chrome on Android prior to 92.0.4515.107 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2021-30585	Use after free in sensor handling in Google Chrome on Windows prior to 92.0.4515.107 allowed a remote

	attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30588	Type confusion in V8 in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30589	Insufficient validation of untrusted input in Sharing in Google Chrome prior to 92.0.4515.107 allowed a remote attacker to bypass navigation restrictions via a crafted click-to-call link.
CVE-2021-30590	Heap buffer overflow in Bookmarks in Google Chrome prior to 92.0.4515.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30591	Use after free in File System API in Google Chrome prior to 92.0.4515.131 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30592	Out of bounds write in Tab Groups in Google Chrome prior to 92.0.4515.131 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory write via a crafted HTML page.
CVE-2021-30593	Out of bounds read in Tab Strip in Google Chrome prior to 92.0.4515.131 allowed an attacker who convinced a user to install a malicious extension to perform an out of bounds memory read via a crafted HTML page.
CVE-2021-30594	Use after free in Page Info UI in Google Chrome prior to 92.0.4515.131 allowed a remote attacker to potentially exploit heap corruption via physical access to the device.
CVE-2021-30596	Incorrect security UI in Navigation in Google Chrome on Android prior to 92.0.4515.131 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2021-30597	Use after free in Browser UI in Google Chrome on Chrome prior to 92.0.4515.131 allowed a remote attacker to potentially exploit heap corruption via physical access to the device.
CVE-2021-30598	Type confusion in V8 in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2021-30599	Type confusion in V8 in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2021-30600	Use after free in Printing in Google Chrome prior to 92.0.4515.159 allowed a remote attacker who had

	compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30601	Use after free in Extensions API in Google Chrome prior to 92.0.4515.159 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30602	Use after free in WebRTC in Google Chrome prior to 92.0.4515.159 allowed an attacker who convinced a user to visit a malicious website to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30603	Data race in WebAudio in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30604	Use after free in ANGLE in Google Chrome prior to 92.0.4515.159 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30606	Chromium: CVE-2021-30606 Use after free in Blink
CVE-2021-30607	Chromium: CVE-2021-30607 Use after free in Permissions
CVE-2021-30608	Chromium: CVE-2021-30608 Use after free in Web Share
CVE-2021-30609	Chromium: CVE-2021-30609 Use after free in Sign-In
CVE-2021-30610	Chromium: CVE-2021-30610 Use after free in Extensions API
CVE-2021-30611	Chromium: CVE-2021-30611 Use after free in WebRTC
CVE-2021-30612	Chromium: CVE-2021-30612 Use after free in WebRTC
CVE-2021-30613	Chromium: CVE-2021-30613 Use after free in Base internals
CVE-2021-30614	Chromium: CVE-2021-30614 Heap buffer overflow in TabStrip
CVE-2021-30615	Chromium: CVE-2021-30615 Cross-origin data leak in Navigation
CVE-2021-30616	Chromium: CVE-2021-30616 Use after free in Media
CVE-2021-30617	Chromium: CVE-2021-30617 Policy bypass in Blink
CVE-2021-30618	Chromium: CVE-2021-30618 Inappropriate implementation in DevTools
CVE-2021-30619	Chromium: CVE-2021-30619 UI Spoofing in Autofill
CVE-2021-30620	Chromium: CVE-2021-30620 Insufficient policy enforcement in Blink
CVE-2021-30621	Chromium: CVE-2021-30621 UI Spoofing in Autofill
CVE-2021-30622	Chromium: CVE-2021-30622 Use after free in WebApp Installs
CVE-2021-30623	Chromium: CVE-2021-30623 Use after free in Bookmarks

CVE-2021-30624	Chromium: CVE-2021-30624 Use after free in Autofill
CVE-2021-30625	Use after free in Selection API in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who convinced the user to visit a malicious website to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30626	Out of bounds memory access in ANGLE in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30627	Type confusion in Blink layout in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30628	Stack buffer overflow in ANGLE in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit stack corruption via a crafted HTML page.
CVE-2021-30629	Use after free in Permissions in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30630	Inappropriate implementation in Blink in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page.
CVE-2021-30632	Out of bounds write in V8 in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-30633	Use after free in Indexed DB API in Google Chrome prior to 93.0.4577.82 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-30641	Apache HTTP Server versions 2.4.39 to 2.4.46 Unexpected matching behavior with 'MergeSlashes OFF'
CVE-2021-30858	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 14.8 and iPadOS 14.8, macOS Big Sur 11.6. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.
CVE-2021-3100	The Apache Log4j hotpatch package before log4j-cve-2021-44228-hotpatch-1.1-13 didn't mimic the permissions of the JVM being patched, allowing it to escalate privileges.
CVE-2021-3114	In Go before 1.14.14 and 1.15.x before 1.15.7, crypto/elliptic/p224.go can generate incorrect outputs, related to an underflow of the lowest limb during the final complete reduction in the P-224 field.

CVE-2021-3115	Go before 1.14.14 and 1.15.x before 1.15.7 on Windows is vulnerable to Command Injection and remote code execution when using the "go get" command to fetch modules that make use of cgo (for example, cgo can execute a gcc program from an untrusted download).
CVE-2021-31162	In the standard library in Rust before 1.52.0, a double free can occur in the Vec::from_iter function if freeing the element panics.
CVE-2021-31440	This vulnerability allows local attackers to escalate privileges on affected installations of Linux Kernel 5.11.15. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. The specific flaw exists within the handling of eBPF programs. The issue results from the lack of proper validation of user-supplied eBPF programs prior to executing them. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the kernel. Was ZDI-CAN-13661.
CVE-2021-31525	net/http in Go before 1.15.12 and 1.16.x before 1.16.4 allows remote attackers to cause a denial of service (panic) via a large header to ReadRequest or ReadResponse. Server, Transport, and Client can each be affected in some configurations.
CVE-2021-31535	LookupCol.c in X.Org X through X11R7.7 and libX11 before 1.7.1 might allow remote attackers to execute arbitrary code. The libX11 XLookupColor request (intended for server-side color lookup) contains a flaw allowing a client to send color-name requests with a name longer than the maximum size allowed by the protocol (and also longer than the maximum packet size for normal-sized packets). The user-controlled data exceeding the maximum size is then interpreted by the server as additional X protocol requests and executed, e.g., to disable X server authorization completely. For example, if the victim encounters malicious terminal control sequences for color codes, then the attacker may be able to take full control of the running graphical session.
CVE-2021-3156	Sudo before 1.9.5p2 contains an off-by-one error that can result in a heap-based buffer overflow, which allows privilege escalation to root via "sudoedit -s" and a command-line argument that ends with a single backslash character.
CVE-2021-31618	Apache HTTP Server protocol handler for the HTTP/2 protocol checks received request headers against the size limitations as configured for the server and used for the HTTP/1 protocol as well. On violation of these restrictions and HTTP response is sent to the client with a status code indicating why the request was rejected.

	This rejection response was not fully initialised in the HTTP/2 protocol handler if the offending header was the very first one received or appeared in a footer. This led to a NULL pointer dereference on initialised memory, crashing reliably the child process. Since such a triggering HTTP/2 request is easy to craft and submit, this can be exploited to DoS the server. This issue affected mod_http2 1.15.17 and Apache HTTP Server version 2.4.47 only. Apache HTTP Server 2.4.47 was never released.
CVE-2021-3177	Python 3.x through 3.9.1 has a buffer overflow in PyCArg_repr in _ctypes/callproc.c, which may lead to remote code execution in certain Python applications that accept floating-point numbers as untrusted input, as demonstrated by a 1e300 argument to c_double.from_param. This occurs because sprintf is used unsafely.
CVE-2021-3178	** DISPUTED ** fs/nfsd/nfs3xdr.c in the Linux kernel through 5.10.8, when there is an NFS export of a subdirectory of a filesystem, allows remote attackers to traverse to other parts of the filesystem via REaddirplus. NOTE: some parties argue that such a subdirectory export is not intended to prevent this attack; see also the exports(5) no_subtree_check default behavior.
CVE-2021-31829	kernel/bpf/verifier.c in the Linux kernel through 5.12.1 performs undesirable speculative loads, leading to disclosure of stack content via side-channel attacks, aka CID-801c6058d14a. The specific concern is not protecting the BPF stack area against speculative loads. Also, the BPF stack can contain uninitialized data that might represent sensitive information previously operated on by the kernel.
CVE-2021-32399	net/bluetooth/hci_request.c in the Linux kernel through 5.12.2 has a race condition for removal of the HCI controller.
CVE-2021-3246	A heap buffer overflow vulnerability in msadpcm_decode_block of libsndfile 1.0.30 allows attackers to execute arbitrary code via a crafted WAV file.
CVE-2021-32610	In Archive_Tar before 1.4.14, symlinks can refer to targets outside of the extracted archive, a different vulnerability than CVE-2020-36193.
CVE-2021-32760	containerd is a container runtime. A bug was found in containerd versions prior to 1.4.8 and 1.5.4 where pulling and extracting a specially-crafted container image can result in Unix file permission changes for existing files in the host's filesystem. Changes to file permissions can deny access to the expected owner of the file, widen access to others, or set extended bits like setuid, setgid, and sticky. This bug does not

	directly allow files to be read, modified, or executed without an additional cooperating process. This bug has been fixed in containerd 1.5.4 and 1.4.8. As a workaround, ensure that users only pull images from trusted sources. Linux security modules (LSMs) like SELinux and AppArmor can limit the files potentially affected by this bug through policies and profiles that prevent containerd from interacting with specific files.
CVE-2021-32810	crossbeam-deque is a package of work-stealing deques for building task schedulers when programming in Rust. In versions prior to 0.7.4 and 0.8.0, the result of the race condition is that one or more tasks in the worker queue can be popped twice instead of other tasks that are forgotten and never popped. If tasks are allocated on the heap, this can cause double free and a memory leak. If not, this still can cause a logical bug. Crates using `Stealer::steal`, `Stealer::steal_batch`, or `Stealer::steal_batch_and_pop` are affected by this issue. This has been fixed in crossbeam-deque 0.8.1 and 0.7.4.
CVE-2021-33034	In the Linux kernel before 5.12.4, net/bluetooth/hci_event.c has a use-after-free when destroying an hci_chan, aka CID-5c4c8c954409. This leads to writing an arbitrary value.
CVE-2021-33193	A crafted method sent through HTTP/2 will bypass validation and be forwarded by mod_proxy, which can lead to request splitting or cache poisoning. This issue affects Apache HTTP Server 2.4.17 to 2.4.48.
CVE-2021-33195	In archive/zip in Go before 1.15.13 and 1.16.x before 1.16.5 has functions for DNS lookups that do not validate replies from DNS servers, and thus a return value may contain an unsafe injection (e.g., XSS) that does not conform to the RFC1035 format.
CVE-2021-33196	In archive/zip in Go before 1.15.13 and 1.16.x before 1.16.5, a crafted file count (in an archive's header) can cause a NewReader or OpenReader panic.
CVE-2021-33197	In Go before 1.15.13 and 1.16.x before 1.16.5, some configurations of ReverseProxy (from net/http/httputil) result in a situation where an attacker is able to drop arbitrary headers.
CVE-2021-33198	In Go before 1.15.13 and 1.16.x before 1.16.5, there can be a panic for a large exponent to the math/big.Rat SetString or UnmarshalText method.
CVE-2021-33200	kernel/bpf/verifier.c in the Linux kernel through 5.12.7 enforces incorrect limits for pointer arithmetic operations, aka CID-bb01a1bba579. This can be abused to perform out-of-bounds reads and writes in kernel memory, leading to local privilege escalation to root. In particular, there is a corner case where the off

	reg causes a masking direction change, which then results in an incorrect final aux->alu_limit.
CVE-2021-3326	The iconv function in the GNU C Library (aka glibc or libc6) 2.32 and earlier, when processing invalid input sequences in the ISO-2022-JP-3 encoding, fails an assertion in the code path and aborts the program, potentially resulting in a denial of service.
CVE-2021-3347	An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault handling, allowing local users to execute code in the kernel, aka CID-34b1a1ce1458.
CVE-2021-3348	nbd_add_socket in drivers/block/nbd.c in the Linux kernel through 5.10.12 has an ndb_queue_rq use-after-free that could be triggered by local attackers (with access to the nbd device) via an I/O request at a certain point during device setup, aka CID-b98e762e3d71.
CVE-2021-33503	An issue was discovered in urllib3 before 1.26.5. When provided with a URL containing many @ characters in the authority component, the authority regular expression exhibits catastrophic backtracking, causing a denial of service if a URL were passed as a parameter or redirected to via an HTTP redirect.
CVE-2021-33516	An issue was discovered in GUPnP before 1.0.7 and 1.1.x and 1.2.x before 1.2.5. It allows DNS rebinding. A remote web server can exploit this vulnerability to trick a victim's browser into triggering actions against local UPnP services implemented using this library. Depending on the affected service, this could be used for data exfiltration, data tempering, etc.
CVE-2021-33560	Libgcrypt before 1.8.8 and 1.9.x before 1.9.3 mishandles ElGamal encryption because it lacks exponent blinding to address a side-channel attack against mpi_powm, and the window size is not chosen appropriately. This, for example, affects use of ElGamal in OpenPGP.
CVE-2021-33574	The mq_notify function in the GNU C Library (aka glibc) versions 2.32 and 2.33 has a use-after-free. It may use the notification thread attributes object (passed through its struct sigevent parameter) after it has been freed by the caller, leading to a denial of service (application crash) or possibly unspecified other impact.
CVE-2021-33582	Cyrus IMAP before 3.4.2 allows remote attackers to cause a denial of service (multiple-minute daemon hang) via input that is mishandled during hash-table interaction. Because there are many insertions into a single bucket, strcmp becomes slow. This is fixed in 3.4.2, 3.2.8, and 3.0.16.
CVE-2021-33624	In kernel/bpf/verifier.c in the Linux kernel before 5.12.13, a branch can be mispredicted (e.g., because of type confusion) and consequently an unprivileged BPF

	program can read arbitrary memory locations via a side-channel attack, aka CID-9183671af6db.
CVE-2021-33655	When sending malicious data to kernel by ioctl cmd FBIOPUT_VSCREENINFO, kernel will write memory out of bounds.
CVE-2021-33909	fs/seq_file.c in the Linux kernel 3.16 through 5.13.x before 5.13.4 does not properly restrict seq buffer allocations, leading to an integer overflow, an Out-of-bounds Write, and escalation to root by an unprivileged user, aka CID-8cae8cd89f05.
CVE-2021-3421	A flaw was found in the RPM package in the read functionality. This flaw allows an attacker who can convince a victim to install a seemingly verifiable package or compromise an RPM repository, to cause RPM database corruption. The highest threat from this vulnerability is to data integrity. This flaw affects RPM versions before 4.17.0-alpha.
CVE-2021-3426	There's a flaw in Python 3's pydoc. A local or adjacent attacker who discovers or is able to convince another local or adjacent user to start a pydoc server could access the server and use it to disclose sensitive information belonging to the other user that they would not normally be able to access. The highest risk of this flaw is to data confidentiality. This flaw affects Python versions before 3.8.9, Python versions before 3.9.3 and Python versions before 3.10.0a7.
CVE-2021-3429	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2021-34423	A buffer overflow vulnerability was discovered in Zoom Client for Meetings (for Android, iOS, Linux, macOS, and Windows) before version 5.8.4, Zoom Client for Meetings for Blackberry (for Android and iOS) before version 5.8.1, Zoom Client for Meetings for intune (for Android and iOS) before version 5.8.4, Zoom Client for Meetings for Chrome OS before version 5.0.1, Zoom Rooms for Conference Room (for Android, AndroidBali, macOS, and Windows) before version 5.8.3, Controllers for Zoom Rooms (for Android, iOS, and Windows) before version 5.8.3, Zoom VDI Windows Meeting Client before version 5.8.4, Zoom VDI Azure Virtual Desktop Plugins (for Windows x86 or x64, IGEL x64, Ubuntu x64, HP ThinPro OS x64) before version 5.8.4.21112, Zoom VDI Citrix Plugins (for Windows x86 or x64, Mac Universal Installer & Uninstaller, IGEL x64, eLux RP6 x64, HP ThinPro OS x64, Ubuntu x64, CentOS x 64, Dell ThinOS) before version 5.8.4.21112, Zoom VDI VMware Plugins (for Windows x86 or x64, Mac Universal Installer & Uninstaller, IGEL x64, eLux

	<p>RP6 x64, HP ThinPro OS x64, Ubuntu x64, CentOS x 64, Dell ThinOS) before version 5.8.4.21112, Zoom Meeting SDK for Android before version 5.7.6.1922, Zoom Meeting SDK for iOS before version 5.7.6.1082, Zoom Meeting SDK for macOS before version 5.7.6.1340, Zoom Meeting SDK for Windows before version 5.7.6.1081, Zoom Video SDK (for Android, iOS, macOS, and Windows) before version 1.1.2, Zoom On-Premise Meeting Connector Controller before version 4.8.12.20211115, Zoom On-Premise Meeting Connector MMR before version 4.8.12.20211115, Zoom On-Premise Recording Connector before version 5.1.0.65.20211116, Zoom On-Premise Virtual Room Connector before version 4.4.7266.20211117, Zoom On-Premise Virtual Room Connector Load Balancer before version 2.5.5692.20211117, Zoom Hybrid Zproxy before version 1.0.1058.20211116, and Zoom Hybrid MMR before version 4.6.20211116.131_x86-64. This can potentially allow a malicious actor to crash the service or application, or leverage this vulnerability to execute arbitrary code.</p>
CVE-2021-34424	<p>A vulnerability was discovered in the Zoom Client for Meetings (for Android, iOS, Linux, macOS, and Windows) before version 5.8.4, Zoom Client for Meetings for Blackberry (for Android and iOS) before version 5.8.1, Zoom Client for Meetings for intune (for Android and iOS) before version 5.8.4, Zoom Client for Meetings for Chrome OS before version 5.0.1, Zoom Rooms for Conference Room (for Android, AndroidBali, macOS, and Windows) before version 5.8.3, Controllers for Zoom Rooms (for Android, iOS, and Windows) before version 5.8.3, Zoom VDI Windows Meeting Client before version 5.8.4, Zoom VDI Azure Virtual Desktop Plugins (for Windows x86 or x64, IGEL x64, Ubuntu x64, HP ThinPro OS x64) before version 5.8.4.21112, Zoom VDI Citrix Plugins (for Windows x86 or x64, Mac Universal Installer & Uninstaller, IGEL x64, eLux RP6 x64, HP ThinPro OS x64, Ubuntu x64, CentOS x 64, Dell ThinOS) before version 5.8.4.21112, Zoom VDI VMware Plugins (for Windows x86 or x64, Mac Universal Installer & Uninstaller, IGEL x64, eLux RP6 x64, HP ThinPro OS x64, Ubuntu x64, CentOS x 64, Dell ThinOS) before version 5.8.4.21112, Zoom Meeting SDK for Android before version 5.7.6.1922, Zoom Meeting SDK for iOS before version 5.7.6.1082, Zoom Meeting SDK for macOS before version 5.7.6.1340, Zoom Meeting SDK for Windows before version 5.7.6.1081, Zoom Video SDK (for Android, iOS, macOS, and Windows) before version 1.1.2, Zoom on-premise Meeting Connector before version 4.8.12.20211115, Zoom on-premise Meeting Connector MMR before version 4.8.12.20211115, Zoom on-premise Recording Connector before version</p>

	5.1.0.65.20211116, Zoom on-premise Virtual Room Connector before version 4.4.7266.20211117, Zoom on-premise Virtual Room Connector Load Balancer before version 2.5.5692.20211117, Zoom Hybrid Zproxy before version 1.0.1058.20211116, and Zoom Hybrid MMR before version 4.6.20211116.131_x86-64 which potentially allowed for the exposure of the state of process memory. This issue could be used to potentially gain insight into arbitrary areas of the product's memory.
CVE-2021-3449	An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension (where it was present in the initial ClientHello), but includes a signature_algorithms_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration). OpenSSL TLS clients are not impacted by this issue. All OpenSSL 1.1.1 versions are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL 1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1-1.1.1j).
CVE-2021-3450	The X509_V_FLAG_X509_STRICT flag enables additional security checks of the certificates present in a certificate chain. It is not set by default. Starting from OpenSSL version 1.1.1h a check to disallow certificates in the chain that have explicitly encoded elliptic curve parameters was added as an additional strict check. An error in the implementation of this check meant that the result of a previous check to confirm that certificates in the chain are valid CA certificates was overwritten. This effectively bypasses the check that non-CA certificates must not be able to issue other certificates. If a "purpose" has been configured then there is a subsequent opportunity for checks that the certificate is a valid CA. All of the named "purpose" values implemented in libcrypto perform this check. Therefore, where a purpose is set the certificate chain will still be rejected even when the strict flag has been used. A purpose is set by default in libssl client and server certificate verification routines, but it can be overridden or removed by an application. In order to be affected, an application must explicitly set the X509_V_FLAG_X509_STRICT verification flag and either not set a purpose for the certificate verification or, in the case of TLS client or server applications, override the default purpose. OpenSSL versions 1.1.1h and newer are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1k. OpenSSL

	1.0.2 is not impacted by this issue. Fixed in OpenSSL 1.1.1k (Affected 1.1.1h-1.1.1j).
CVE-2021-34556	In the Linux kernel through 5.13.7, an unprivileged BPF program can obtain sensitive information from kernel memory via a Speculative Store Bypass side-channel attack because the protection mechanism neglects the possibility of uninitialized memory locations on the BPF stack.
CVE-2021-34558	The crypto/tls package of Go through 1.16.5 does not properly assert that the type of public key in an X.509 certificate matches the expected type when doing a RSA based key exchange, allowing a malicious TLS server to cause a TLS client to panic.
CVE-2021-34693	net/can/bcm.c in the Linux kernel through 5.12.10 allows local users to obtain sensitive information from kernel stack memory because parts of a data structure are uninitialized.
CVE-2021-3472	A flaw was found in xorg-x11-server in versions before 1.20.11. An integer underflow can occur in xserver which can lead to a local privilege escalation. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-34798	Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVE-2021-3480	A flaw was found in slapi-nis in versions before 0.56.7. A NULL pointer dereference during the parsing of the Binding DN could allow an unauthenticated attacker to crash the 389-ds-base directory server. The highest threat from this vulnerability is to system availability.
CVE-2021-3483	A flaw was found in the Nosy driver in the Linux kernel. This issue allows a device to be inserted twice into a doubly-linked list, leading to a use-after-free when one of these devices is removed. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability. Versions before kernel 5.12-rc6 are affected
CVE-2021-3487	There's a flaw in the BFD library of binutils in versions before 2.36. An attacker who supplies a crafted file to an application linked with BFD, and using the DWARF functionality, could cause an impact to system availability by way of excessive memory consumption.
CVE-2021-3489	The eBPF RINGBUF bpf_ringbuf_reserve() function in the Linux kernel did not check that the allocated size was smaller than the ringbuf size, allowing an attacker to perform out-of-bounds writes within the kernel and therefore, arbitrary code execution. This issue was fixed via commit 4b81ccebaeee ("bpf, ringbuf: Deny reserve of buffers larger than ringbuf") (v5.13-rc4) and

	backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. It was introduced via 457f44363a88 ("bpf: Implement BPF ring buffer and verifier support for it") (v5.8-rc1).
CVE-2021-3490	The eBPF ALU32 bounds tracking for bitwise ops (AND, OR and XOR) in the Linux kernel did not properly update 32-bit bounds, which could be turned into out of bounds reads and writes in the Linux kernel and therefore, arbitrary code execution. This issue was fixed via commit 049c4e13714e ("bpf: Fix alu32 const subreg bound tracking on bitwise operations") (v5.13-rc4) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. The AND/OR issues were introduced by commit 3f50f132d840 ("bpf: Verifier, do explicit ALU32 bounds tracking") (5.7-rc1) and the XOR variant was introduced by 2921c90d4718 ("bpf:Fix a verifier failure with xor") (5.10-rc1).
CVE-2021-3491	The io_uring subsystem in the Linux kernel allowed the MAX_RW_COUNT limit to be bypassed in the PROVIDE_BUFFERS operation, which led to negative values being used in mem_rw when reading /proc/<PID>/mem. This could be used to create a heap overflow leading to arbitrary code execution in the kernel. It was addressed via commit d1f82808877b ("io_uring: truncate lengths larger than MAX_RW_COUNT on provide buffers") (v5.13-rc1) and backported to the stable kernels in v5.12.4, v5.11.21, and v5.10.37. It was introduced in ddf0322db79c ("io_uring: add IORING_OP_PROVIDE_BUFFERS") (v5.7-rc1).
CVE-2021-3501	A flaw was found in the Linux kernel in versions before 5.12. The value of internal.ndata, in the KVM API, is mapped to an array index, which can be updated by a user process at anytime which could lead to an out-of-bounds write. The highest threat from this vulnerability is to data integrity and system availability.
CVE-2021-3504	A flaw was found in the hivex library in versions before 1.3.20. It is caused due to a lack of bounds check within the hivex_open function. An attacker could input a specially crafted Windows Registry (hive) file which would cause hivex to read memory beyond its normal bounds or cause the program to crash. The highest threat from this vulnerability is to system availability.
CVE-2021-3506	An out-of-bounds (OOB) memory access flaw was found in fs/f2fs/node.c in the f2fs module in the Linux kernel in versions before 5.12.0-rc4. A bounds check failure allows a local attacker to gain access to out-of-bounds memory leading to a system crash or a leak of internal kernel information. The highest threat from this vulnerability is to system availability.

CVE-2021-3516	There's a flaw in libxml2's xmllint in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by xmllint could trigger a use-after-free. The greatest impact of this flaw is to confidentiality, integrity, and availability.
CVE-2021-3517	There is a flaw in the xml entity encoding functionality of libxml2 in versions before 2.9.11. An attacker who is able to supply a crafted file to be processed by an application linked with the affected functionality of libxml2 could trigger an out-of-bounds read. The most likely impact of this flaw is to application availability, with some potential impact to confidentiality and integrity if an attacker is able to use memory information to further exploit the application.
CVE-2021-3518	There's a flaw in libxml2 in versions before 2.9.11. An attacker who is able to submit a crafted file to be processed by an application linked with libxml2 could trigger a use-after-free. The greatest impact from this flaw is to confidentiality, integrity, and availability.
CVE-2021-3522	GStreamer before 1.18.4 may perform an out-of-bounds read when handling certain ID3v2 tags.
CVE-2021-3537	A vulnerability found in libxml2 in versions before 2.9.11 shows that it did not propagate errors while parsing XML mixed content, causing a NULL dereference. If an untrusted XML document was parsed in recovery mode and post-validated, the flaw could be used to crash the application. The highest threat from this vulnerability is to system availability.
CVE-2021-3541	A flaw was found in libxml2. Exponential entity expansion attack its possible bypassing all existing protection mechanisms and leading to denial of service.
CVE-2021-3543	A flaw null pointer dereference in the Nitro Enclaves kernel driver was found in the way that Enclaves VMs forces closures on the enclave file descriptor. A local user of a host machine could use this flaw to crash the system or escalate their privileges on the system.
CVE-2021-35477	In the Linux kernel through 5.13.7, an unprivileged BPF program can obtain sensitive information from kernel memory via a Speculative Store Bypass side-channel attack because a certain preempting store operation does not necessarily occur before a store operation that has an attacker-controlled value.
CVE-2021-35550	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks

	<p>of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).</p>
CVE-2021-35556	<p>Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).</p>
CVE-2021-35559	<p>Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Swing). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. 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 can also be</p>

	exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2021-35560	Vulnerability in the Java SE product of Oracle Java SE (component: Deployment). The supported version that is affected is Java SE: 8u301. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.1 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).
CVE-2021-35561	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Utility). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2021-35564	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Keytool). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily

	<p>exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).</p>
CVE-2021-35565	<p>Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).</p>
CVE-2021-35567	<p>Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows low privileged attacker with network access via Kerberos to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Oracle GraalVM Enterprise Edition, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and</p>

	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 3.1 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:N/A:N).
CVE-2021-35578	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2021-35586	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2021-35588	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Java SE: 7u311, 8u301; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via

	<p>multiple protocols to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L).</p>
CVE-2021-35603	Vulnerability in the Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JSSE). Supported versions that are affected are Java SE: 7u311, 8u301, 11.0.12, 17; Oracle GraalVM Enterprise Edition: 20.3.3 and 21.2.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via TLS to compromise Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2021-3561	An Out of Bounds flaw was found fig2dev version 3.2.8a. A flawed bounds check in read_objects() could allow an attacker to provide a crafted malicious input causing the application to either crash or in some cases cause memory corruption. The highest threat from this vulnerability is to integrity as well as system availability.
CVE-2021-3564	A flaw double-free memory corruption in the Linux kernel HCI device initialization subsystem was found in the way user attach malicious HCI TTY Bluetooth device. A local user could use this flaw to crash the system. This flaw affects all the Linux kernel versions starting from 3.13.
CVE-2021-3570	A flaw was found in the ptpt4l program of the linuxptp package. A missing length check when forwarding a

	PTP message between ports allows a remote attacker to cause an information leak, crash, or potentially remote code execution. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. This flaw affects linuxptp versions before 3.1.1, before 2.0.1, before 1.9.3, before 1.8.1, before 1.7.1, before 1.6.1 and before 1.5.1.
CVE-2021-3571	A flaw was found in the ptpt4l program of the linuxptp package. When ptpt4l is operating on a little-endian architecture as a PTP transparent clock, a remote attacker could send a crafted one-step sync message to cause an information leak or crash. The highest threat from this vulnerability is to data confidentiality and system availability. This flaw affects linuxptp versions before 3.1.1 and before 2.0.1.
CVE-2021-3572	A flaw was found in python-pip in the way it handled Unicode separators in git references. A remote attacker could possibly use this issue to install a different revision on a repository. The highest threat from this vulnerability is to data integrity. This is fixed in python-pip version 21.1.
CVE-2021-3573	A use-after-free in function hci_sock_bound_ioctl() of the Linux kernel HCI subsystem was found in the way user calls ioctl HCIUNBLOCKADDR or other way triggers race condition of the call hci_unregister_dev() together with one of the calls hci_sock_blacklist_add(), hci_sock_blacklist_del(), hci_get_conn_info(), hci_get_auth_info(). A privileged local user could use this flaw to crash the system or escalate their privileges on the system. This flaw affects the Linux kernel versions prior to 5.13-rc5.
CVE-2021-3575	A heap-based buffer overflow was found in openjpeg in color.c:379:42 in sycc420_to_rgb when decompressing a crafted .j2k file. An attacker could use this to execute arbitrary code with the permissions of the application compiled against openjpeg.
CVE-2021-35942	The wordexp function in the GNU C Library (aka glibc) through 2.33 may crash or read arbitrary memory in parse_param (in posix/wordexp.c) when called with an untrusted, crafted pattern, potentially resulting in a denial of service or disclosure of information. This occurs because atoi was used but strtol should have been used to ensure correct calculations.
CVE-2021-36160	A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This issue affects Apache HTTP Server versions 2.4.30 to 2.4.48 (inclusive).
CVE-2021-3621	A flaw was found in SSSD, where the sssctl command was vulnerable to shell command injection via the logs-fetch and cache-expire subcommands. This flaw allows an attacker to trick the root user into running a specially

	crafted sssctl command, such as via sudo, to gain root access. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.
CVE-2021-3622	A flaw was found in the hivex library. This flaw allows an attacker to input a specially crafted Windows Registry (hive) file, which would cause hivex to recursively call the _get_children() function, leading to a stack overflow. The highest threat from this vulnerability is to system availability.
CVE-2021-36221	Go before 1.15.15 and 1.16.x before 1.16.7 has a race condition that can lead to a net/http/httpputil ReverseProxy panic upon an ErrAbortHandler abort.
CVE-2021-3640	A flaw use-after-free in function sco_sock_sendmsg() of the Linux kernel HCI subsystem was found in the way user calls iocet UFFDIO_REGISTER or other way triggers race condition of the call sco_conn_del() together with the call sco_sock_sendmsg() with the expected controllable faulting memory page. A privileged local user could use this flaw to crash the system or escalate their privileges on the system.
CVE-2021-3652	A flaw was found in 389-ds-base. If an asterisk is imported as password hashes, either accidentally or maliciously, then instead of being inactive, any password will successfully match during authentication. This flaw allows an attacker to successfully authenticate as a user whose password was disabled.
CVE-2021-3653	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "int_ctl" field, this issue could allow a malicious L1 to enable AVIC support (Advanced Virtual Interrupt Controller) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape. This flaw affects Linux kernel versions prior to 5.14-rc7.
CVE-2021-3655	A vulnerability was found in the Linux kernel in versions prior to v5.14-rc1. Missing size validations on inbound SCTP packets may allow the kernel to read uninitialized memory.
CVE-2021-3656	A flaw was found in the KVM's AMD code for supporting SVM nested virtualization. The flaw occurs when processing the VMCB (virtual machine control block) provided by the L1 guest to spawn/handle a nested guest (L2). Due to improper validation of the "virt_ext" field, this issue could allow a malicious L1 to disable both VMLOAD/VMSAVE intercepts and VLS (Virtual VMLOAD/VMSAVE) for the L2 guest. As a result, the L2 guest would be allowed to read/write physical pages

	of the host, resulting in a crash of the entire system, leak of sensitive data or potential guest-to-host escape.
CVE-2021-3679	A lack of CPU resource in the Linux kernel tracing module functionality in versions prior to 5.14-rc3 was found in the way user uses trace ring buffer in a specific way. Only privileged local users (with CAP_SYS_ADMIN capability) could use this flaw to starve the resources causing denial of service.
CVE-2021-3712	ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are represented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).
CVE-2021-37159	hso_free_net_device in drivers/net/usb/hso.c in the Linux kernel through 5.13.4 calls unregister_netdev

	without checking for the NETREG_REGISTERED state, leading to a use-after-free and a double free.
CVE-2021-3732	A security issue was found in Linux kernel's OverlayFS subsystem where a local attacker who has the ability to mount the TmpFS filesystem with OverlayFS can abuse a logic bug in the overlayfs code which can inadvertently reveal files hidden in the original mount.
CVE-2021-3733	There's a flaw in urllib's AbstractBasicAuthHandler class. An attacker who controls a malicious HTTP server that an HTTP client (such as web browser) connects to, could trigger a Regular Expression Denial of Service (ReDOS) during an authentication request with a specially crafted payload that is sent by the server to the client. The greatest threat that this flaw poses is to application availability.
CVE-2021-3737	A flaw was found in python. An improperly handled HTTP response in the HTTP client code of python may allow a remote attacker, who controls the HTTP server, to make the client script enter an infinite loop, consuming CPU time. The highest threat from this vulnerability is to system availability.
CVE-2021-3739	A NULL pointer dereference flaw was found in the btrfs_rm_device function in fs/btrfs/volumes.c in the Linux Kernel, where triggering the bug requires 'CAP_SYS_ADMIN'. This flaw allows a local attacker to crash the system or leak kernel internal information. The highest threat from this vulnerability is to system availability.
CVE-2021-3744	A memory leak flaw was found in the Linux kernel in the ccp_run_aes_gcm_cmd() function in drivers/crypto/ccp/ccp-ops.c, which allows attackers to cause a denial of service (memory consumption). This vulnerability is similar with the older CVE-2019-18808.
CVE-2021-3753	A race problem was seen in the vt_k_ioctl in drivers/tty/vt/vt_ioctl.c in the Linux kernel, which may cause an out of bounds read in vt as the write access to vc_mode is not protected by lock-in vt_ioctl (KDSETMDE). The highest threat from this vulnerability is to data confidentiality.
CVE-2021-3764	A memory leak flaw was found in the Linux kernel's ccp_run_aes_gcm_cmd() function that allows an attacker to cause a denial of service. The vulnerability is similar to the older CVE-2019-18808. The highest threat from this vulnerability is to system availability.
CVE-2021-3772	A flaw was found in the Linux SCTP stack. A blind attacker may be able to kill an existing SCTP association through invalid chunks if the attacker knows the IP-addresses and port numbers being used and the attacker can send packets with spoofed IP addresses.

CVE-2021-37750	The Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.18.5 and 1.19.x before 1.19.3 has a NULL pointer dereference in kdc/do_tgs_req.c via a FAST inner body that lacks a server field.
CVE-2021-3778	vim is vulnerable to Heap-based Buffer Overflow
CVE-2021-37956	Use after free in Offline use in Google Chrome on Android prior to 94.0.4606.54 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37957	Use after free in WebGPU in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37958	Inappropriate implementation in Navigation in Google Chrome on Windows prior to 94.0.4606.54 allowed a remote attacker to inject scripts or HTML into a privileged page via a crafted HTML page.
CVE-2021-37959	Use after free in Task Manager in Google Chrome prior to 94.0.4606.54 allowed an attacker who convinced a user to engage in a series of user gestures to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-3796	vim is vulnerable to Use After Free
CVE-2021-37961	Use after free in Tab Strip in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37962	Use after free in Performance Manager in Google Chrome prior to 94.0.4606.54 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37963	Side-channel information leakage in DevTools in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2021-37964	Inappropriate implementation in ChromeOS Networking in Google Chrome on ChromeOS prior to 94.0.4606.54 allowed an attacker with a rogue wireless access point to potentially carryout a wifi impersonation attack via a crafted ONC file.
CVE-2021-37965	Inappropriate implementation in Background Fetch API in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-37966	Inappropriate implementation in Compositing in Google Chrome on Android prior to 94.0.4606.54 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.

CVE-2021-37967	Inappropriate implementation in Background Fetch API in Google Chrome prior to 94.0.4606.54 allowed a remote attacker who had compromised the renderer process to leak cross-origin data via a crafted HTML page.
CVE-2021-37968	Inappropriate implementation in Background Fetch API in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-37969	Inappropriate implementation in Google Updater in Google Chrome on Windows prior to 94.0.4606.54 allowed a remote attacker to perform local privilege escalation via a crafted file.
CVE-2021-37970	Use after free in File System API in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37971	Incorrect security UI in Web Browser UI in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2021-37972	Out of bounds read in libjpeg-turbo in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37973	Use after free in Portals in Google Chrome prior to 94.0.4606.61 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-37974	Use after free in Safebrowsing in Google Chrome prior to 94.0.4606.71 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37975	Use after free in V8 in Google Chrome prior to 94.0.4606.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37976	Inappropriate implementation in Memory in Google Chrome prior to 94.0.4606.71 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2021-37977	Use after free in Garbage Collection in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37978	Heap buffer overflow in Blink in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37979	heap buffer overflow in WebRTC in Google Chrome prior to 94.0.4606.81 allowed a remote attacker who

	convinced a user to browse to a malicious website to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37980	Inappropriate implementation in Sandbox in Google Chrome prior to 94.0.4606.81 allowed a remote attacker to potentially bypass site isolation via Windows.
CVE-2021-37981	Heap buffer overflow in Skia in Google Chrome prior to 95.0.4638.54 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-37982	Use after free in Incognito in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37983	Use after free in Dev Tools in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37984	Heap buffer overflow in PDFium in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37985	Use after free in V8 in Google Chrome prior to 95.0.4638.54 allowed a remote attacker who had convinced a user to allow for connection to debugger to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37986	Heap buffer overflow in Settings in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to engage with Dev Tools to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37987	Use after free in Network APIs in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37988	Use after free in Profiles in Google Chrome prior to 95.0.4638.54 allowed a remote attacker who convinced a user to engage in specific gestures to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37989	Inappropriate implementation in Blink in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to abuse content security policy via a crafted HTML page.
CVE-2021-37990	Inappropriate implementation in WebView in Google Chrome on Android prior to 95.0.4638.54 allowed a remote attacker to leak cross-origin data via a crafted app.
CVE-2021-37991	Race in V8 in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2021-37992	Out of bounds read in WebAudio in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37993	Use after free in PDF Accessibility in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37994	Inappropriate implementation in iFrame Sandbox in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2021-37995	Inappropriate implementation in WebApp Installer in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to potentially overlay and spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2021-37996	Insufficient validation of untrusted input Downloads in Google Chrome prior to 95.0.4638.54 allowed a remote attacker to bypass navigation restrictions via a malicious file.
CVE-2021-37997	Use after free in Sign-In in Google Chrome prior to 95.0.4638.69 allowed a remote attacker who convinced a user to sign into Chrome to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37998	Use after free in Garbage Collection in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-37999	Insufficient data validation in New Tab Page in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to inject arbitrary scripts or HTML in a new browser tab via a crafted HTML page.
CVE-2021-38000	Insufficient validation of untrusted input in Intents in Google Chrome on Android prior to 95.0.4638.69 allowed a remote attacker to arbitrarily browser to a malicious URL via a crafted HTML page.
CVE-2021-38001	Type confusion in V8 in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-38002	Use after free in Web Transport in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-38003	Inappropriate implementation in V8 in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2021-38004	Insufficient policy enforcement in Autofill in Google Chrome prior to 95.0.4638.69 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-38005	Use after free in loader in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-38006	Use after free in storage foundation in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-38007	Type confusion in V8 in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-38008	Use after free in media in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-38009	Inappropriate implementation in cache in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-38010	Inappropriate implementation in service workers in Google Chrome prior to 96.0.4664.45 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.
CVE-2021-38011	Use after free in storage foundation in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-38012	Type confusion in V8 in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-38013	Heap buffer overflow in fingerprint recognition in Google Chrome on ChromeOS prior to 96.0.4664.45 allowed a remote attacker who had compromised a WebUI renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-38014	Out of bounds write in Swiftshader in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-38015	Inappropriate implementation in input in Google Chrome prior to 96.0.4664.45 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted Chrome Extension.
CVE-2021-38016	Insufficient policy enforcement in background fetch in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to bypass same origin policy via a crafted HTML page.

CVE-2021-38017	Insufficient policy enforcement in iframe sandbox in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2021-38018	Inappropriate implementation in navigation in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2021-38019	Insufficient policy enforcement in CORS in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-38020	Insufficient policy enforcement in contacts picker in Google Chrome on Android prior to 96.0.4664.45 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2021-38021	Inappropriate implementation in referrer in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2021-38022	Inappropriate implementation in WebAuthentication in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-38160	** DISPUTED ** In drivers/char/virtio_console.c in the Linux kernel before 5.13.4, data corruption or loss can be triggered by an untrusted device that supplies a buf->len value exceeding the buffer size. NOTE: the vendor indicates that the cited data corruption is not a vulnerability in any existing use case; the length validation was added solely for robustness in the face of anomalous host OS behavior.
CVE-2021-38166	In kernel/bpf/hashtab.c in the Linux kernel through 5.13.8, there is an integer overflow and out-of-bounds write when many elements are placed in a single bucket. NOTE: exploitation might be impractical without the CAP_SYS_ADMIN capability.
CVE-2021-38198	arch/x86/kvm/mmu/paging_tmpl.h in the Linux kernel before 5.12.11 incorrectly computes the access permissions of a shadow page, leading to a missing guest protection page fault.
CVE-2021-38199	fs/nfs/nfs4client.c in the Linux kernel before 5.13.4 has incorrect connection-setup ordering, which allows operators of remote NFSv4 servers to cause a denial of service (hanging of mounts) by arranging for those servers to be unreachable during trunking detection.
CVE-2021-38208	net/nfc/llcp_sock.c in the Linux kernel before 5.12.10 allows local unprivileged users to cause a denial of service (NULL pointer dereference and BUG) by making a getsockname call after a certain type of failure of a bind call.

CVE-2021-38297	Go before 1.16.9 and 1.17.x before 1.17.2 has a Buffer Overflow via large arguments in a function invocation from a WASM module, when GOARCH=wasm GOOS=js is used.
CVE-2021-38300	arch/mips/net/bpf_jit.c in the Linux kernel before 5.4.10 can generate undesirable machine code when transforming unprivileged cBPF programs, allowing execution of arbitrary code within the kernel context. This occurs because conditional branches can exceed the 128 KB limit of the MIPS architecture.
CVE-2021-38493	Mozilla developers reported memory safety bugs present in Firefox 91 and Firefox ESR 78.13. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 78.14, Thunderbird < 78.14, and Firefox < 92.
CVE-2021-38495	Mozilla developers reported memory safety bugs present in Thunderbird 78.13.0. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 91.1 and Firefox ESR < 91.1.
CVE-2021-38496	During operations on MessageTasks, a task may have been removed while it was still scheduled, resulting in memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR < 91.2, Firefox ESR < 78.15, and Firefox < 93.
CVE-2021-38497	Through use of reportValidity() and window.open(), a plain-text validation message could have been overlaid on another origin, leading to possible user confusion and spoofing attacks. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 91.2.
CVE-2021-38498	During process shutdown, a document could have caused a use-after-free of a languages service object, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 91.2.
CVE-2021-38500	Mozilla developers reported memory safety bugs present in Firefox 92 and Firefox ESR 91.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 78.15, Thunderbird < 91.2, Firefox ESR < 91.2, Firefox ESR < 78.15, and Firefox < 93.
CVE-2021-38501	Mozilla developers reported memory safety bugs present in Firefox 92 and Firefox ESR 91.1. Some of

	these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 93, Thunderbird < 91.2, and Firefox ESR < 91.2.
CVE-2021-38502	Thunderbird ignored the configuration to require STARTTLS security for an SMTP connection. A MITM could perform a downgrade attack to intercept transmitted messages, or could take control of the authenticated session to execute SMTP commands chosen by the MITM. If an unprotected authentication method was configured, the MITM could obtain the authentication credentials, too. This vulnerability affects Thunderbird < 91.2.
CVE-2021-38645	Open Management Infrastructure Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-38648, CVE-2021-38649.
CVE-2021-38647	Open Management Infrastructure Remote Code Execution Vulnerability
CVE-2021-38648	Open Management Infrastructure Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-38645, CVE-2021-38649.
CVE-2021-38649	Open Management Infrastructure Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021-38645, CVE-2021-38648.
CVE-2021-3872	vim is vulnerable to Heap-based Buffer Overflow
CVE-2021-3875	vim is vulnerable to Heap-based Buffer Overflow
CVE-2021-3903	vim is vulnerable to Heap-based Buffer Overflow
CVE-2021-39139	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. A user is only affected if using the version out of the box with JDK 1.7u21 or below. However, this scenario can be adjusted easily to an external Xalan that works regardless of the version of the Java runtime. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.
CVE-2021-39140	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to allocate 100% CPU time on the target system depending on CPU type or parallel execution of such a payload resulting in a denial of service only by manipulating the processed input stream. No user is affected, who followed

	the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.
CVE-2021-39141	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.
CVE-2021-39144	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker has sufficient rights to execute commands of the host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.
CVE-2021-39145	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.
CVE-2021-39146	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.
CVE-2021-39147	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's

	security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.
CVE-2021-39148	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.
CVE-2021-39149	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.
CVE-2021-39150	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to request data from internal resources that are not publicly available only by manipulating the processed input stream with a Java runtime version 14 to 8. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the [Security Framework](https://x-stream.github.io/security.html#framework), you will have to use at least version 1.4.18.
CVE-2021-39151	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.
CVE-2021-39152	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to request data from internal resources that are not publicly available only by manipulating the processed input stream with a

	Java runtime version 14 to 8. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. If you rely on XStream's default blacklist of the [Security Framework](https://x-stream.github.io/security.html#framework), you will have to use at least version 1.4.18.
CVE-2021-39153	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream, if using the version out of the box with Java runtime version 14 to 8 or with JavaFX installed. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.
CVE-2021-39154	XStream is a simple library to serialize objects to XML and back again. In affected versions this vulnerability may allow a remote attacker to load and execute arbitrary code from a remote host only by manipulating the processed input stream. No user is affected, who followed the recommendation to setup XStream's security framework with a whitelist limited to the minimal required types. XStream 1.4.18 uses no longer a blacklist by default, since it cannot be secured for general purpose.
CVE-2021-3927	vim is vulnerable to Heap-based Buffer Overflow
CVE-2021-39275	ap_escape_quotes() may write beyond the end of a buffer when given malicious input. No included modules pass untrusted data to these functions, but third-party / external modules may. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVE-2021-3928	vim is vulnerable to Use of Uninitialized Variable
CVE-2021-39293	In archive/zip in Go before 1.16.8 and 1.17.x before 1.17.1, a crafted archive header (falsely designating that many files are present) can cause a NewReader or OpenReader panic. NOTE: this issue exists because of an incomplete fix for CVE-2021-33196.
CVE-2021-3968	vim is vulnerable to Heap-based Buffer Overflow
CVE-2021-3973	vim is vulnerable to Heap-based Buffer Overflow
CVE-2021-3974	vim is vulnerable to Use After Free
CVE-2021-3981	A flaw in grub2 was found where its configuration file, known as grub.cfg, is being created with the wrong permission set allowing non privileged users to read its content. This represents a low severity confidentiality issue, as those users can eventually read

	any encrypted passwords present in grub.cfg. This flaw affects grub2 2.06 and previous versions. This issue has been fixed in grub upstream but no version with the fix is currently released.
CVE-2021-3984	vim is vulnerable to Heap-based Buffer Overflow
CVE-2021-4001	A race condition was found in the Linux kernel's ebpf verifier between bpf_map_update_elem and bpf_map_freeze due to a missing lock in kernel/bpf/syscall.c. In this flaw, a local user with a special privilege (cap_sys_admin or cap_bpf) can modify the frozen mapped address space. This flaw affects kernel versions prior to 5.16 rc2.
CVE-2021-4002	A memory leak flaw in the Linux kernel's hugetlbfs memory usage was found in the way the user maps some regions of memory twice using shmget() which are aligned to PUD alignment with the fault of some of the memory pages. A local user could use this flaw to get unauthorized access to some data.
CVE-2021-4008	A flaw was found in xorg-x11-server in versions before 21.1.2 and before 1.20.14. An out-of-bounds access can occur in the SProcRenderCompositeGlyphs function. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-4009	A flaw was found in xorg-x11-server in versions before 21.1.2 and before 1.20.14. An out-of-bounds access can occur in the SProcXFixesCreatePointerBarrier function. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-4010	A flaw was found in xorg-x11-server in versions before 21.1.2 and before 1.20.14. An out-of-bounds access can occur in the SProcScreenSaverSuspend function. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-4011	A flaw was found in xorg-x11-server in versions before 21.1.2 and before 1.20.14. An out-of-bounds access can occur in the SwapCreateRegister function. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.
CVE-2021-4019	vim is vulnerable to Heap-based Buffer Overflow
CVE-2021-4034	A local privilege escalation vulnerability was found on polkit's pkexec utility. The pkexec application is a setuid tool designed to allow unprivileged users to run commands as privileged users according predefined policies. The current version of pkexec doesn't handle the calling parameters count correctly and ends trying to execute environment variables as commands. An

	attacker can leverage this by crafting environment variables in such a way it'll induce pkexec to execute arbitrary code. When successfully executed the attack can cause a local privilege escalation given unprivileged users administrative rights on the target machine.
CVE-2021-40438	A crafted request uri-path can cause mod_proxy to forward the request to an origin server chosen by the remote user. This issue affects Apache HTTP Server 2.4.48 and earlier.
CVE-2021-40490	A race condition was discovered in ext4_write_inline_data_end in fs/ext4/inline.c in the ext4 subsystem in the Linux kernel through 5.13.13.
CVE-2021-4052	Use after free in web apps in Google Chrome prior to 96.0.4664.93 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2021-4053	Use after free in UI in Google Chrome on Linux prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-4054	Incorrect security UI in autofill in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2021-4055	Heap buffer overflow in extensions in Google Chrome prior to 96.0.4664.93 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2021-4056	Type confusion in loader in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-4057	Use after free in file API in Google Chrome prior to 96.0.4664.93 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-4058	Heap buffer overflow in ANGLE in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-4059	Insufficient data validation in loader in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-4061	Type confusion in V8 in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-4062	Heap buffer overflow in BFCache in Google Chrome prior to 96.0.4664.93 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.

CVE-2021-4063	Use after free in developer tools in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-4064	Use after free in screen capture in Google Chrome on ChromeOS prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-4065	Use after free in autofill in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-4066	Integer underflow in ANGLE in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-4067	Use after free in window manager in Google Chrome on ChromeOS prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-4068	Insufficient data validation in new tab page in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2021-4069	vim is vulnerable to Use After Free
CVE-2021-4078	Type confusion in V8 in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-4079	Out of bounds write in WebRTC in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to potentially exploit heap corruption via crafted WebRTC packets.
CVE-2021-4083	A read-after-free memory flaw was found in the Linux kernel's garbage collection for Unix domain socket file handlers in the way users call close() and fget() simultaneously and can potentially trigger a race condition. This flaw allows a local user to crash the system or escalate their privileges on the system. This flaw affects Linux kernel versions prior to 5.16-rc4.
CVE-2021-4091	A double-free was found in the way 389-ds-base handles virtual attributes context in persistent searches. An attacker could send a series of search requests, forcing the server to behave unexpectedly, and crash.
CVE-2021-4098	Insufficient data validation in Mojo in Google Chrome prior to 96.0.4664.110 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2021-4099	Use after free in Swiftshader in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-4100	Object lifecycle issue in ANGLE in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to

	potentially exploit heap corruption via a crafted HTML page.
CVE-2021-4101	Heap buffer overflow in Swiftshader in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-4102	Use after free in V8 in Google Chrome prior to 96.0.4664.110 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2021-4104	JMSAppender in Log4j 1.2 is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration. The attacker can provide TopicBindingName and TopicConnectionFactoryBindingName configurations causing JMSAppender to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-44228. Note this issue only affects Log4j 1.2 when specifically configured to use JMSAppender, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.
CVE-2021-41073	loop_rw_iter in fs/io_uring.c in the Linux kernel 5.10 through 5.14.6 allows local users to gain privileges by using IORING_OP_PROVIDE_BUFFERS to trigger a free of a kernel buffer, as demonstrated by using /proc/<pid>/maps for exploitation.
CVE-2021-41089	Moby is an open-source project created by Docker to enable software containerization. A bug was found in Moby (Docker Engine) where attempting to copy files using `docker cp` into a specially-crafted container can result in Unix file permission changes for existing files in the host's filesystem, widening access to others. This bug does not directly allow files to be read, modified, or executed without an additional cooperating process. This bug has been fixed in Moby (Docker Engine) 20.10.9. Users should update to this version as soon as possible. Running containers do not need to be restarted.
CVE-2021-41091	Moby is an open-source project created by Docker to enable software containerization. A bug was found in Moby (Docker Engine) where the data directory (typically `/var/lib/docker`) contained subdirectories with insufficiently restricted permissions, allowing otherwise unprivileged Linux users to traverse directory contents and execute programs. When containers included executable programs with extended permission bits (such as `setuid`), unprivileged Linux users could discover and execute those programs. When the UID of an unprivileged Linux user on the host collided with the file owner or group inside a container, the unprivileged

	Linux user on the host could discover, read, and modify those files. This bug has been fixed in Moby (Docker Engine) 20.10.9. Users should update to this version as soon as possible. Running containers should be stopped and restarted for the permissions to be fixed. For users unable to upgrade limit access to the host to trusted users. Limit access to host volumes to trusted containers.
CVE-2021-41092	Docker CLI is the command line interface for the docker container runtime. A bug was found in the Docker CLI where running `docker login my-private-registry.example.com` with a misconfigured configuration file (typically `~/.docker/config.json`) listing a `credsStore` or `credHelpers` that could not be executed would result in any provided credentials being sent to `registry-1.docker.io` rather than the intended private registry. This bug has been fixed in Docker CLI 20.10.9. Users should update to this version as soon as possible. For users unable to update ensure that any configured credsStore or credHelpers entries in the configuration file reference an installed credential helper that is executable and on the PATH.
CVE-2021-41103	containerd is an open source container runtime with an emphasis on simplicity, robustness and portability. A bug was found in containerd where container root directories and some plugins had insufficiently restricted permissions, allowing otherwise unprivileged Linux users to traverse directory contents and execute programs. When containers included executable programs with extended permission bits (such as setuid), unprivileged Linux users could discover and execute those programs. When the UID of an unprivileged Linux user on the host collided with the file owner or group inside a container, the unprivileged Linux user on the host could discover, read, and modify those files. This vulnerability has been fixed in containerd 1.4.11 and containerd 1.5.7. Users should update to these versions when they are released and may restart containers or update directory permissions to mitigate the vulnerability. Users unable to update should limit access to the host to trusted users. Update directory permission on container bundles directories.
CVE-2021-41159	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. All FreeRDP clients prior to version 2.4.1 using gateway connections (`/gt:rpc`) fail to validate input data. A malicious gateway might allow client memory to be written out of bounds. This issue has been resolved in version 2.4.1. If you are unable to update then use `/gt:http` rather than /gt:rdp connections if possible or use a direct connection without a gateway.

CVE-2021-41160	FreeRDP is a free implementation of the Remote Desktop Protocol (RDP), released under the Apache license. In affected versions a malicious server might trigger out of bound writes in a connected client. Connections using GDI or SurfaceCommands to send graphics updates to the client might send '0' width/ height or out of bound rectangles to trigger out of bound writes. With '0' width or height the memory allocation will be '0' but the missing bounds checks allow writing to the pointer at this (not allocated) region. This issue has been patched in FreeRDP 2.4.1.
CVE-2021-41190	The OCI Distribution Spec project defines an API protocol to facilitate and standardize the distribution of content. In the OCI Distribution Specification version 1.0.0 and prior, the Content-Type header alone was used to determine the type of document during push and pull operations. Documents that contain both "manifests" and "layers" fields could be interpreted as either a manifest or an index in the absence of an accompanying Content-Type header. If a Content-Type header changed between two pulls of the same digest, a client may interpret the resulting content differently. The OCI Distribution Specification has been updated to require that a mediaType value present in a manifest or index match the Content-Type header used during the push and pull operations. Clients pulling from a registry may distrust the Content-Type header and reject an ambiguous document that contains both "manifests" and "layers" fields or "manifests" and "config" fields if they are unable to update to version 1.0.1 of the spec.
CVE-2021-4135	A memory leak vulnerability was found in the Linux kernel's eBPF for the Simulated networking device driver in the way user uses BPF for the device such that function nsim_map_alloc_elem being called. A local user could use this flaw to get unauthorized access to some data.
CVE-2021-4136	vim is vulnerable to Heap-based Buffer Overflow
CVE-2021-41524	While fuzzing the 2.4.49 httpd, a new null pointer dereference was detected during HTTP/2 request processing, allowing an external source to DoS the server. This requires a specially crafted request. The vulnerability was recently introduced in version 2.4.49. No exploit is known to the project.
CVE-2021-4155	A data leak flaw was found in the way XFS_IOC_ALLOCSP IOCTL in the XFS filesystem allowed for size increase of files with unaligned size. A local attacker could use this flaw to leak data on the XFS filesystem otherwise not accessible to them.
CVE-2021-41617	sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental

	groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.
CVE-2021-4166	vim is vulnerable to Out-of-bounds Read
CVE-2021-4173	vim is vulnerable to Use After Free
CVE-2021-41771	ImportedSymbols in debug/macho (for Open or OpenFat) in Go before 1.16.10 and 1.17.x before 1.17.3 Accesses a Memory Location After the End of a Buffer, aka an out-of-bounds slice situation.
CVE-2021-41772	Go before 1.16.10 and 1.17.x before 1.17.3 allows an archive/zip Reader.Open panic via a crafted ZIP archive containing an invalid name or an empty filename field.
CVE-2021-41773	A flaw was found in a change made to path normalization in Apache HTTP Server 2.4.49. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased paths, this could allow for remote code execution. This issue is known to be exploited in the wild. This issue only affects Apache 2.4.49 and not earlier versions. The fix in Apache HTTP Server 2.4.50 was found to be incomplete, see CVE-2021-42013.
CVE-2021-41864	prealloc_elems_and_freelist in kernel/bpf/stackmap.c in the Linux kernel before 5.14.12 allows unprivileged users to trigger an eBPF multiplication integer overflow with a resultant out-of-bounds write.
CVE-2021-4187	vim is vulnerable to Use After Free
CVE-2021-4189	A flaw was found in Python, specifically in the FTP (File Transfer Protocol) client library in PASV (passive) mode. The issue is how the FTP client trusts the host from the PASV response by default. This flaw allows an attacker to set up a malicious FTP server that can trick FTP clients into connecting back to a given IP address and port. This vulnerability could lead to FTP client scanning ports, which otherwise would not have been possible.
CVE-2021-4192	vim is vulnerable to Use After Free
CVE-2021-4193	vim is vulnerable to Out-of-bounds Read
CVE-2021-4197	An unprivileged write to the file handler flaw in the Linux kernel's control groups and namespaces subsystem was found in the way users have access to some less privileged process that are controlled by cgroups and have higher privileged parent process. It is actually both

	for cgroup2 and cgroup1 versions of control groups. A local user could use this flaw to crash the system or escalate their privileges on the system.
CVE-2021-42013	It was found that the fix for CVE-2021-41773 in Apache HTTP Server 2.4.50 was insufficient. An attacker could use a path traversal attack to map URLs to files outside the directories configured by Alias-like directives. If files outside of these directories are not protected by the usual default configuration "require all denied", these requests can succeed. If CGI scripts are also enabled for these aliased pathes, this could allow for remote code execution. This issue only affects Apache 2.4.49 and Apache 2.4.50 and not earlier versions.
CVE-2021-42097	GNU Mailman before 2.1.35 may allow remote Privilege Escalation. A csrf_token value is not specific to a single user account. An attacker can obtain a value within the context of an unprivileged user account, and then use that value in a CSRF attack against an admin (e.g., for account takeover).
CVE-2021-42325	Froxlor through 0.10.29.1 allows SQL injection in Database/Manager/DbManagerMySQL.php via a custom DB name.
CVE-2021-42574	** DISPUTED ** An issue was discovered in the Bidirectional Algorithm in the Unicode Specification through 14.0. It permits the visual reordering of characters via control sequences, which can be used to craft source code that renders different logic than the logical ordering of tokens ingested by compilers and interpreters. Adversaries can leverage this to encode source code for compilers accepting Unicode such that targeted vulnerabilities are introduced invisibly to human reviewers. NOTE: the Unicode Consortium offers the following alternative approach to presenting this concern. An issue is noted in the nature of international text that can affect applications that implement support for The Unicode Standard and the Unicode Bidirectional Algorithm (all versions). Due to text display behavior when text includes left-to-right and right-to-left characters, the visual order of tokens may be different from their logical order. Additionally, control characters needed to fully support the requirements of bidirectional text can further obfuscate the logical order of tokens. Unless mitigated, an adversary could craft source code such that the ordering of tokens perceived by human reviewers does not match what will be processed by a compiler/interpreter/etc. The Unicode Consortium has documented this class of vulnerability in its document, Unicode Technical Report #36, Unicode Security Considerations. The Unicode Consortium also provides guidance on mitigations for this class of issues in Unicode Technical Standard #39, Unicode Security Mechanisms, and in Unicode

	Standard Annex #31, Unicode Identifier and Pattern Syntax. Also, the BIDI specification allows applications to tailor the implementation in ways that can mitigate misleading visual reordering in program text; see HL4 in Unicode Standard Annex #9, Unicode Bidirectional Algorithm.
CVE-2021-43267	An issue was discovered in net/tipc/crypto.c in the Linux kernel before 5.14.16. The Transparent Inter-Process Communication (TIPC) functionality allows remote attackers to exploit insufficient validation of user-supplied sizes for the MSG_CRYPTO message type.
CVE-2021-43527	NSS (Network Security Services) versions prior to 3.73 or 3.68.1 ESR are vulnerable to a heap overflow when handling DER-encoded DSA or RSA-PSS signatures. Applications using NSS for handling signatures encoded within CMS, S/MIME, PKCS \#7, or PKCS \#12 are likely to be impacted. Applications using NSS for certificate validation or other TLS, X.509, OCSP or CRL functionality may be impacted, depending on how they configure NSS. *Note: This vulnerability does NOT impact Mozilla Firefox.* However, email clients and PDF viewers that use NSS for signature verification, such as Thunderbird, LibreOffice, Evolution and Evince are believed to be impacted. This vulnerability affects NSS < 3.73 and NSS < 3.68.1.
CVE-2021-43975	In the Linux kernel through 5.15.2, hw_atl_utils_fw_rpc_wait in drivers/net/ethernet/aquantia/atlantic/hw_atl/hw_atl_utils.c allows an attacker (who can introduce a crafted device) to trigger an out-of-bounds write via a crafted length value.
CVE-2021-44077	Zoho ManageEngine ServiceDesk Plus before 11306, ServiceDesk Plus MSP before 10530, and SupportCenter Plus before 11014 are vulnerable to unauthenticated remote code execution. This is related to /RestAPI URLs in a servlet, and ImportTechnicians in the Struts configuration.
CVE-2021-44142	The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP files server." Samba versions prior to 4.13.17, 4.14.12 and 4.15.5 with vfs_fruit configured allow out-of-bounds heap read and write via specially crafted extended file attributes. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.
CVE-2021-44224	A crafted URI sent to httpd configured as a forward proxy (ProxyRequests on) can cause a crash (NULL pointer dereference) or, for configurations mixing forward and reverse proxy declarations, can allow for requests to be directed to a declared Unix Domain

	Socket endpoint (Server Side Request Forgery). This issue affects Apache HTTP Server 2.4.7 up to 2.4.51 (included).
CVE-2021-44227	In GNU Mailman before 2.1.38, a list member or moderator can get a CSRF token and craft an admin request (using that token) to set a new admin password or make other changes.
CVE-2021-44228	Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages, and parameters do not protect against attacker controlled LDAP and other JNDI related endpoints. An attacker who can control log messages or log message parameters can execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled. From log4j 2.15.0, this behavior has been disabled by default. From version 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely removed. Note that this vulnerability is specific to log4j-core and does not affect log4net, log4cxx, or other Apache Logging Services projects.
CVE-2021-44521	When running Apache Cassandra with the following configuration: enable_user_defined_functions: true enable_scripted_user_defined_functions: true enable_user_defined_functions_threads: false it is possible for an attacker to execute arbitrary code on the host. The attacker would need to have enough permissions to create user defined functions in the cluster to be able to exploit this. Note that this configuration is documented as unsafe, and will continue to be considered unsafe after this CVE.
CVE-2021-44716	net/http in Go before 1.16.12 and 1.17.x before 1.17.5 allows uncontrolled memory consumption in the header canonicalization cache via HTTP/2 requests.
CVE-2021-44717	Go before 1.16.12 and 1.17.x before 1.17.5 on UNIX allows write operations to an unintended file or unintended network connection as a consequence of erroneous closing of file descriptor 0 after file-descriptor exhaustion.
CVE-2021-44733	A use-after-free exists in drivers/tee/tee_shm.c in the TEE subsystem in the Linux kernel through 5.15.11. This occurs because of a race condition in tee_shm_get_from_id during an attempt to free a shared memory object.
CVE-2021-44790	A carefully crafted request body can cause a buffer overflow in the mod_lua multipart parser (r:parsebody() called from Lua scripts). The Apache httpd team is not aware of an exploit for the vulnerability though it might be possible to craft one. This issue affects Apache HTTP Server 2.4.51 and earlier.

CVE-2021-44832	Apache Log4j2 versions 2.0-beta7 through 2.17.0 (excluding security fix releases 2.3.2 and 2.12.4) are vulnerable to a remote code execution (RCE) attack when a configuration uses a JDBC Appender with a JNDI LDAP data source URI when an attacker has control of the target LDAP server. This issue is fixed by limiting JNDI data source names to the java protocol in Log4j2 versions 2.17.1, 2.12.4, and 2.3.2.
CVE-2021-45046	It was found that the fix to address CVE-2021-44228 in Apache Log4j 2.15.0 was incomplete in certain non-default configurations. This could allow attackers with control over Thread Context Map (MDC) input data when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, \$\$\{ctx:loginId\}) or a Thread Context Map pattern (%X, %mdc, or %MDC) to craft malicious input data using a JNDI Lookup pattern resulting in an information leak and remote code execution in some environments and local code execution in all environments. Log4j 2.16.0 (Java 8) and 2.12.2 (Java 7) fix this issue by removing support for message lookup patterns and disabling JNDI functionality by default.
CVE-2021-45095	pep_sock_accept in net/phonet/pep.c in the Linux kernel through 5.15.8 has a refcount leak.
CVE-2021-45105	Apache Log4j2 versions 2.0-alpha1 through 2.16.0 (excluding 2.12.3 and 2.3.1) did not protect from uncontrolled recursion from self-referential lookups. This allows an attacker with control over Thread Context Map data to cause a denial of service when a crafted string is interpreted. This issue was fixed in Log4j 2.17.0, 2.12.3, and 2.3.1.
CVE-2021-45444	In zsh before 5.8.1, an attacker can achieve code execution if they control a command output inside the prompt, as demonstrated by a %F argument. This occurs because of recursive PROMPT_SUBST expansion.
CVE-2021-45463	load_cache in GEGL before 0.4.34 allows shell expansion when a pathname in a constructed command line is not escaped or filtered. This is caused by use of the system library function for execution of the ImageMagick convert fallback in magick-load. NOTE: GEGL releases before 0.4.34 are used in GIMP releases before 2.10.30; however, this does not imply that GIMP builds enable the vulnerable feature.
CVE-2021-45960	In Expat (aka libexpat) before 2.4.3, a left shift by 29 (or more) places in the storeAttrs function in xmlparse.c can lead to realloc misbehavior (e.g., allocating too few bytes, or only freeing memory).

CVE-2021-46143	In doProlog in xmlparse.c in Expat (aka libexpat) before 2.4.3, an integer overflow exists for m_groupSize.
CVE-2022-0001	Non-transparent sharing of branch predictor selectors between contexts in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.
CVE-2022-0002	Non-transparent sharing of branch predictor within a context in some Intel(R) Processors may allow an authorized user to potentially enable information disclosure via local access.
CVE-2022-0070	Incomplete fix for CVE-2021-3100. The Apache Log4j hotpatch package starting with log4j-cve-2021-44228-hotpatch-1.1-16 will now explicitly mimic the Linux capabilities and cgroups of the target Java process that the hotpatch is applied to.
CVE-2022-0096	Use after free in Storage in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0097	Inappropriate implementation in DevTools in Google Chrome prior to 97.0.4692.71 allowed an attacker who convinced a user to install a malicious extension to potentially allow extension to escape the sandbox via a crafted HTML page.
CVE-2022-0098	Use after free in Screen Capture in Google Chrome on Chrome OS prior to 97.0.4692.71 allowed an attacker who convinced a user to perform specific user gestures to potentially exploit heap corruption via specific user gestures.
CVE-2022-0099	Use after free in Sign-in in Google Chrome prior to 97.0.4692.71 allowed a remote attacker who convinced a user to perform specific user gestures to potentially exploit heap corruption via specific user gesture.
CVE-2022-0100	Heap buffer overflow in Media streams API in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0101	Heap buffer overflow in Bookmarks in Google Chrome prior to 97.0.4692.71 allowed a remote attacker who convinced a user to perform specific user gesture to potentially exploit heap corruption via specific user gesture.
CVE-2022-0102	Type confusion in V8 in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0103	Use after free in SwiftShader in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2022-0104	Heap buffer overflow in ANGLE in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0105	Use after free in PDF Accessibility in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0106	Use after free in Autofill in Google Chrome prior to 97.0.4692.71 allowed a remote attacker who convinced a user to perform specific user gesture to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0107	Use after free in File Manager API in Google Chrome on Chrome OS prior to 97.0.4692.71 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0108	Inappropriate implementation in Navigation in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2022-0109	Inappropriate implementation in Autofill in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to obtain potentially sensitive information via a crafted HTML page.
CVE-2022-0110	Incorrect security UI in Autofill in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2022-0111	Inappropriate implementation in Navigation in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to incorrectly set origin via a crafted HTML page.
CVE-2022-0112	Incorrect security UI in Browser UI in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to display missing URL or incorrect URL via a crafted URL.
CVE-2022-0113	Inappropriate implementation in Blink in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2022-0114	Out of bounds memory access in Blink Serial API in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page and virtual serial port driver.
CVE-2022-0115	Uninitialized use in File API in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2022-0116	Inappropriate implementation in Compositing in Google Chrome prior to 97.0.4692.71 allowed a remote attacker

	to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2022-0117	Policy bypass in Blink in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2022-0118	Inappropriate implementation in WebShare in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially hide the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2022-0120	Inappropriate implementation in Passwords in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to potentially leak cross-origin data via a malicious website.
CVE-2022-0156	vim is vulnerable to Use After Free
CVE-2022-0158	vim is vulnerable to Heap-based Buffer Overflow
CVE-2022-0185	A heap-based buffer overflow flaw was found in the way the legacy_parse_param function in the Filesystem Context functionality of the Linux kernel verified the supplied parameters length. An unprivileged (in case of unprivileged user namespaces enabled, otherwise needs namespaced CAP_SYS_ADMIN privilege) local user able to open a filesystem that does not support the Filesystem Context API (and thus fallbacks to legacy handling) could use this flaw to escalate their privileges on the system.
CVE-2022-0213	vim is vulnerable to Heap-based Buffer Overflow
CVE-2022-0261	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.
CVE-2022-0289	Use after free in Safe browsing in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0290	Use after free in Site isolation in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2022-0291	Inappropriate implementation in Storage in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.
CVE-2022-0292	Inappropriate implementation in Fenced Frames in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who had compromised the renderer process to bypass navigation restrictions via a crafted HTML page.
CVE-2022-0293	Use after free in Web packaging in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0294	Inappropriate implementation in Push messaging in Google Chrome prior to 97.0.4692.99 allowed a remote

	attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.
CVE-2022-0295	Use after free in Omnibox in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who convinced the user to engage in specific user interactions to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0296	Use after free in Printing in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who convinced the user to engage in specific user interactions to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0297	Use after free in Vulkan in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0298	Use after free in Scheduling in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0300	Use after free in Text Input Method Editor in Google Chrome on Android prior to 97.0.4692.99 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0301	Heap buffer overflow in DevTools in Google Chrome prior to 97.0.4692.99 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0302	Use after free in Omnibox in Google Chrome prior to 97.0.4692.99 allowed an attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0304	Use after free in Bookmarks in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0305	Inappropriate implementation in Service Worker API in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who had compromised the renderer process to bypass site isolation via a crafted HTML page.
CVE-2022-0306	Heap buffer overflow in PDFium in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0307	Use after free in Optimization Guide in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who convinced a user to engage in specific user interaction

	to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0308	Use after free in Data Transfer in Google Chrome on Chrome OS prior to 97.0.4692.99 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0309	Inappropriate implementation in Autofill in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2022-0310	Heap buffer overflow in Task Manager in Google Chrome prior to 97.0.4692.99 allowed a remote attacker to potentially exploit heap corruption via specific user interactions.
CVE-2022-0311	Heap buffer overflow in Task Manager in Google Chrome prior to 97.0.4692.99 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0318	Heap-based Buffer Overflow in vim/vim prior to 8.2.
CVE-2022-0330	A random memory access flaw was found in the Linux kernel's GPU i915 kernel driver functionality in the way a user may run malicious code on the GPU. This flaw allows a local user to crash the system or escalate their privileges on the system.
CVE-2022-0351	Access of Memory Location Before Start of Buffer in GitHub repository vim/vim prior to 8.2.
CVE-2022-0359	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.
CVE-2022-0391	A flaw was found in Python, specifically within the urllib.parse module. This module helps break Uniform Resource Locator (URL) strings into components. The issue involves how the urlparse method does not sanitize input and allows characters like '\r' and '\n' in the URL path. This flaw allows an attacker to input a crafted URL, leading to injection attacks. This flaw affects Python versions prior to 3.10.0b1, 3.9.5, 3.8.11, 3.7.11 and 3.6.14.
CVE-2022-0393	Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.
CVE-2022-0408	Stack-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.
CVE-2022-0413	Use After Free in GitHub repository vim/vim prior to 8.2.
CVE-2022-0417	Heap-based Buffer Overflow GitHub repository vim/vim prior to 8.2.
CVE-2022-0435	A stack overflow flaw was found in the Linux kernel's TIPC protocol functionality in the way a user sends

	a packet with malicious content where the number of domain member nodes is higher than the 64 allowed. This flaw allows a remote user to crash the system or possibly escalate their privileges if they have access to the TIPC network.
CVE-2022-0443	Use After Free in GitHub repository vim/vim prior to 8.2.
CVE-2022-0452	Use after free in Safe Browsing in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2022-0453	Use after free in Reader Mode in Google Chrome prior to 98.0.4758.80 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0454	Heap buffer overflow in ANGLE in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0455	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 98.0.4758.80 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2022-0456	Use after free in Web Search in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via profile destruction.
CVE-2022-0457	Type confusion in V8 in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0458	Use after free in Thumbnail Tab Strip in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0459	Use after free in Screen Capture in Google Chrome prior to 98.0.4758.80 allowed a remote attacker who had compromised the renderer process and convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0460	Use after free in Window Dialogue in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0461	Policy bypass in COOP in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to bypass iframe sandbox via a crafted HTML page.
CVE-2022-0462	Inappropriate implementation in Scroll in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2022-0463	Use after free in Accessibility in Google Chrome prior to 98.0.4758.80 allowed a remote attacker

	who convinced a user to engage in specific user interaction to potentially exploit heap corruption via user interaction.
CVE-2022-0464	Use after free in Accessibility in Google Chrome prior to 98.0.4758.80 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via user interaction.
CVE-2022-0465	Use after free in Extensions in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via user interaction.
CVE-2022-0466	Inappropriate implementation in Extensions Platform in Google Chrome prior to 98.0.4758.80 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted HTML page.
CVE-2022-0467	Inappropriate implementation in Pointer Lock in Google Chrome on Windows prior to 98.0.4758.80 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2022-0468	Use after free in Payments in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0469	Use after free in Cast in Google Chrome prior to 98.0.4758.80 allowed a remote attacker who convinced a user to engage in specific interactions to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0470	Out of bounds memory access in V8 in Google Chrome prior to 98.0.4758.80 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0492	A vulnerability was found in the Linux kernel's cgroup_release_agent_write in the kernel/cgroup/cgroup-v1.c function. This flaw, under certain circumstances, allows the use of the cgroups v1 release_agent feature to escalate privileges and bypass the namespace isolation unexpectedly.
CVE-2022-0494	A kernel information leak flaw was identified in the scsi_ioctl function in drivers/scsi/scsi_ioctl.c in the Linux kernel. This flaw allows a local attacker with a special user privilege (CAP_SYS_ADMIN or CAP_SYS_RAWIO) to create issues with confidentiality.
CVE-2022-0500	A flaw was found in unrestricted eBPF usage by the BPF_BTF_LOAD, leading to a possible out-of-bounds memory write in the Linux kernel's BPF subsystem due to the way a user loads BTF. This flaw allows a local user to crash or escalate their privileges on the system.

CVE-2022-0554	Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.
CVE-2022-0561	Null source pointer passed as an argument to memcpy() function within TIFFFetchStripThing() in tif_dirread.c in libtiff versions from 3.9.0 to 4.3.0 could lead to Denial of Service via crafted TIFF file. For users that compile libtiff from sources, the fix is available with commit eecb0712.
CVE-2022-0562	Null source pointer passed as an argument to memcpy() function within TIFFReadDirectory() in tif_dirread.c in libtiff versions from 4.0 to 4.3.0 could lead to Denial of Service via crafted TIFF file. For users that compile libtiff from sources, a fix is available with commit 561599c.
CVE-2022-0572	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.
CVE-2022-0603	Use after free in File Manager in Google Chrome on Chrome OS prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0604	Heap buffer overflow in Tab Groups in Google Chrome prior to 98.0.4758.102 allowed an attacker who convinced a user to install a malicious extension and engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0605	Use after free in Webstore API in Google Chrome prior to 98.0.4758.102 allowed an attacker who convinced a user to install a malicious extension and convinced a user to enage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0606	Use after free in ANGLE in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0607	Use after free in GPU in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0608	Integer overflow in Mojo in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0609	Use after free in Animation in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0610	Inappropriate implementation in Gamepad API in Google Chrome prior to 98.0.4758.102 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0617	A flaw null pointer dereference in the Linux kernel UDF file system functionality was found in the way user triggers udf_file_write_iter function for the malicious

	UDF image. A local user could use this flaw to crash the system. Actual from Linux kernel 4.2-rc1 till 5.17-rc2.
CVE-2022-0629	Stack-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.
CVE-2022-0685	Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4418.
CVE-2022-0696	NULL Pointer Dereference in GitHub repository vim/vim prior to 8.2.4428.
CVE-2022-0714	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.4436.
CVE-2022-0729	Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4440.
CVE-2022-0778	The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters. Thus vulnerable situations include: - TLS clients consuming server certificates - TLS servers consuming client certificates - Hosting providers taking certificates or private keys from customers - Certificate authorities parsing certification requests from subscribers - Anything else which parses ASN.1 elliptic curve parameters Also any other applications that use the BN_mod_sqrt() where the attacker can control the parameter values are vulnerable to this DoS issue. In the OpenSSL 1.0.2 version the public key is not parsed during initial parsing of the certificate which makes it slightly harder to trigger the infinite loop. However any operation which requires the public key from the certificate will trigger the infinite loop. In particular the attacker can use a self-signed certificate to trigger the loop during verification of the certificate signature. This issue affects OpenSSL versions 1.0.2, 1.1.1 and 3.0. It was addressed in the releases of 1.1.1n and 3.0.2 on the 15th March 2022. Fixed in OpenSSL 3.0.2 (Affected 3.0.0,3.0.1). Fixed in OpenSSL 1.1.1n (Affected 1.1.1-1.1.1m). Fixed in OpenSSL 1.0.2zd (Affected 1.0.2-1.0.2zc).

CVE-2022-0789	Heap buffer overflow in ANGLE in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0790	Use after free in Cast UI in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially perform a sandbox escape via a crafted HTML page.
CVE-2022-0791	Use after free in Omnibox in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via user interactions.
CVE-2022-0792	Out of bounds read in ANGLE in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0793	Use after free in Cast in Google Chrome prior to 99.0.4844.51 allowed an attacker who convinced a user to install a malicious extension and engage in specific user interaction to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2022-0794	Use after free in WebShare in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0795	Type confusion in Blink Layout in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0796	Use after free in Media in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0797	Out of bounds memory access in Mojo in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2022-0798	Use after free in MediaStream in Google Chrome prior to 99.0.4844.51 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2022-0799	Insufficient policy enforcement in Installer in Google Chrome on Windows prior to 99.0.4844.51 allowed a remote attacker to perform local privilege escalation via a crafted offline installer file.
CVE-2022-0800	Heap buffer overflow in Cast UI in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.

CVE-2022-0802	Inappropriate implementation in Full screen mode in Google Chrome on Android prior to 99.0.4844.51 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2022-0803	Inappropriate implementation in Permissions in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to tamper with the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2022-0804	Inappropriate implementation in Full screen mode in Google Chrome on Android prior to 99.0.4844.51 allowed a remote attacker to hide the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2022-0805	Use after free in Browser Switcher in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via user interaction.
CVE-2022-0806	Data leak in Canvas in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in screen sharing to potentially leak cross-origin data via a crafted HTML page.
CVE-2022-0807	Inappropriate implementation in Autofill in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2022-0808	Use after free in Chrome OS Shell in Google Chrome on Chrome OS prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in a series of user interaction to potentially exploit heap corruption via user interactions.
CVE-2022-0809	Out of bounds memory access in WebXR in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0812	An information leak flaw was found in NFS over RDMA in the net/sunrpc/xprtrdma/rpc_rdma.c in the Linux Kernel. This flaw allows an attacker with normal user privileges to leak kernel information.
CVE-2022-0847	A flaw was found in the way the "flags" member of the new pipe buffer structure was lacking proper initialization in copy_page_to_iter_pipe and push_pipe functions in the Linux kernel and could thus contain stale values. An unprivileged local user could use this flaw to write to pages in the page cache backed by read only files and as such escalate their privileges on the system.
CVE-2022-0854	A memory leak flaw was found in the Linux kernel's DMA subsystem, in the way a user calls

	DMA_FROM_DEVICE. This flaw allows a local user to read random memory from the kernel space.
CVE-2022-0865	Reachable Assertion in tiffcpc in libtiff 4.3.0 allows attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 5e180045.
CVE-2022-0907	Unchecked Return Value to NULL Pointer Dereference in tiffcrop in libtiff 4.3.0 allows attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit f2b656e2.
CVE-2022-0908	Null source pointer passed as an argument to memcpy() function within TIFFFetchNormalTag () in tif_dirread.c in libtiff versions up to 4.3.0 could lead to Denial of Service via crafted TIFF file.
CVE-2022-0909	Divide By Zero error in tiffcrop in libtiff 4.3.0 allows attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit f8d0f9aa.
CVE-2022-0918	A vulnerability was discovered in the 389 Directory Server that allows an unauthenticated attacker with network access to the LDAP port to cause a denial of service. The denial of service is triggered by a single message sent over a TCP connection, no bind or other authentication is required. The message triggers a segmentation fault that results in slapd crashing.
CVE-2022-0924	Out-of-bounds Read error in tiffcpc in libtiff 4.3.0 allows attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 408976c4.
CVE-2022-0943	Heap-based Buffer Overflow occurs in vim in GitHub repository vim/vim prior to 8.2.4563.
CVE-2022-0971	Use after free in Blink Layout in Google Chrome on Android prior to 99.0.4844.74 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0972	Use after free in Extensions in Google Chrome prior to 99.0.4844.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0973	Use after free in Safe Browsing in Google Chrome prior to 99.0.4844.74 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0974	Use after free in Splitscreen in Google Chrome on Chrome OS prior to 99.0.4844.74 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.

CVE-2022-0975	Use after free in ANGLE in Google Chrome prior to 99.0.4844.74 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0976	Heap buffer overflow in GPU in Google Chrome prior to 99.0.4844.74 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0977	Use after free in Browser UI in Google Chrome on Chrome OS prior to 99.0.4844.74 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0978	Use after free in ANGLE in Google Chrome prior to 99.0.4844.74 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0979	Use after free in Safe Browsing in Google Chrome on Android prior to 99.0.4844.74 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-0980	Use after free in New Tab Page in Google Chrome prior to 99.0.4844.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific user interactions.
CVE-2022-0996	A vulnerability was found in the 389 Directory Server that allows expired passwords to access the database to cause improper authentication.
CVE-2022-1011	A use-after-free flaw was found in the Linux kernel's FUSE filesystem in the way a user triggers write(). This flaw allows a local user to gain unauthorized access to data from the FUSE filesystem, resulting in privilege escalation.
CVE-2022-1012	A memory leak problem was found in the TCP source port generation algorithm in net/ipv4/tcp.c due to the small table perturb size. This flaw may allow an attacker to information leak and may cause a denial of service problem.
CVE-2022-1015	A flaw was found in the Linux kernel in linux/net/netfilter/nf_tables_api.c of the netfilter subsystem. This flaw allows a local user to cause an out-of-bounds write issue.
CVE-2022-1016	A flaw was found in the Linux kernel in net/netfilter/nf_tables_core.c:nft_do_chain, which can cause a use-after-free. This issue needs to handle 'return' with proper preconditions, as it can lead to a kernel information leak problem caused by a local, unprivileged attacker.
CVE-2022-1048	A use-after-free flaw was found in the Linux kernel's sound subsystem in the way a user triggers concurrent calls of PCM hw_params. The hw_free ioctls or

	similar race condition happens inside ALSA PCM for other ioctl. This flaw allows a local user to crash or potentially escalate their privileges on the system.
CVE-2022-1096	Type confusion in V8 in Google Chrome prior to 99.0.4844.84 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1125	Use after free in Portals in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via user interaction.
CVE-2022-1127	Use after free in QR Code Generator in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via user interaction.
CVE-2022-1128	Inappropriate implementation in Web Share API in Google Chrome on Windows prior to 100.0.4896.60 allowed an attacker on the local network segment to leak cross-origin data via a crafted HTML page.
CVE-2022-1129	Inappropriate implementation in Full Screen Mode in Google Chrome on Android prior to 100.0.4896.60 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2022-1130	Insufficient validation of trust input in WebOTP in Google Chrome on Android prior to 100.0.4896.60 allowed a remote attacker to send arbitrary intents from any app via a malicious app.
CVE-2022-1131	Use after free in Cast UI in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1132	Inappropriate implementation in Virtual Keyboard in Google Chrome on Chrome OS prior to 100.0.4896.60 allowed a local attacker to bypass navigation restrictions via physical access to the device.
CVE-2022-1133	Use after free in WebRTC Perf in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1134	Type confusion in V8 in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1135	Use after free in Shopping Cart in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to potentially exploit heap corruption via standard feature user interaction.
CVE-2022-1136	Use after free in Tab Strip in Google Chrome prior to 100.0.4896.60 allowed an attacker who convinced a

	user to install a malicious extension to potentially exploit heap corruption via specific set of user gestures.
CVE-2022-1137	Inappropriate implementation in Extensions in Google Chrome prior to 100.0.4896.60 allowed an attacker who convinced a user to install a malicious extension to leak potentially sensitive information via a crafted HTML page.
CVE-2022-1138	Inappropriate implementation in Web Cursor in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who had compromised the renderer process to obscure the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2022-1139	Inappropriate implementation in Background Fetch API in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2022-1141	Use after free in File Manager in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via specific user gesture.
CVE-2022-1142	Heap buffer overflow in WebUI in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via specific input into DevTools.
CVE-2022-1143	Heap buffer overflow in WebUI in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via specific input into DevTools.
CVE-2022-1144	Use after free in WebUI in Google Chrome prior to 100.0.4896.60 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via specific input into DevTools.
CVE-2022-1145	Use after free in Extensions in Google Chrome prior to 100.0.4896.60 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific user interaction and profile destruction.
CVE-2022-1146	Inappropriate implementation in Resource Timing in Google Chrome prior to 100.0.4896.60 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2022-1154	Use after free in utf_ptr2char in GitHub repository vim/vim prior to 8.2.4646.
CVE-2022-1158	A flaw was found in KVM. When updating a guest's page table entry, vm_pgoff was improperly used as the

	offset to get the page's pfn. As vaddr and vm_pgoff are controllable by user-mode processes, this flaw allows unprivileged local users on the host to write outside the userspace region and potentially corrupt the kernel, resulting in a denial of service condition.
CVE-2022-1160	heap buffer overflow in get_one_sourceline in GitHub repository vim/vim prior to 8.2.4647.
CVE-2022-1184	A use-after-free flaw was found in fs/ext4/namei.c:dx_insert_block() in the Linux kernel's filesystem sub-component. This flaw allows a local attacker with a user privilege to cause a denial of service.
CVE-2022-1232	Type confusion in V8 in Google Chrome prior to 100.0.4896.75 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1271	An arbitrary file write vulnerability was found in GNU gzip's zgrep utility. When zgrep is applied on the attacker's chosen file name (for example, a crafted file name), this can overwrite an attacker's content to an arbitrary attacker-selected file. This flaw occurs due to insufficient validation when processing filenames with two or more newlines where selected content and the target file names are embedded in crafted multi-line file names. This flaw allows a remote, low privileged attacker to force zgrep to write arbitrary files on the system.
CVE-2022-1292	The c_rehash script does not properly sanitise shell metacharacters to prevent command injection. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.3 (Affected 3.0.0,3.0.1,3.0.2). Fixed in OpenSSL 1.1.1o (Affected 1.1.1-1.1.1n). Fixed in OpenSSL 1.0.2ze (Affected 1.0.2-1.0.2zd).
CVE-2022-1305	Use after free in storage in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1306	Inappropriate implementation in compositing in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2022-1307	Inappropriate implementation in full screen in Google Chrome on Android prior to 100.0.4896.88 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.

CVE-2022-1308	Use after free in BFCache in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1309	Insufficient policy enforcement in developer tools in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2022-1310	Use after free in regular expressions in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1311	Use after free in shell in Google Chrome on ChromeOS prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1312	Use after free in storage in Google Chrome prior to 100.0.4896.88 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension.
CVE-2022-1313	Use after free in tab groups in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1314	Type confusion in V8 in Google Chrome prior to 100.0.4896.88 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1353	A vulnerability was found in the pfkey_register function in net/key/af_key.c in the Linux kernel. This flaw allows a local, unprivileged user to gain access to kernel memory, leading to a system crash or a leak of internal kernel information.
CVE-2022-1364	Type confusion in V8 Turbofan in Google Chrome prior to 100.0.4896.127 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1381	global heap buffer overflow in skip_range in GitHub repository vim/vim prior to 8.2.4763. This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution
CVE-2022-1420	Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4774.
CVE-2022-1477	Use after free in Vulkan in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1478	Use after free in SwiftShader in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2022-1479	Use after free in ANGLE in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1481	Use after free in Sharing in Google Chrome on Mac prior to 101.0.4951.41 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1482	Inappropriate implementation in WebGL in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1483	Heap buffer overflow in WebGPU in Google Chrome prior to 101.0.4951.41 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1484	Heap buffer overflow in Web UI Settings in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1485	Use after free in File System API in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1486	Type confusion in V8 in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2022-1487	Use after free in Ozone in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via running a Wayland test.
CVE-2022-1488	Inappropriate implementation in Extensions API in Google Chrome prior to 101.0.4951.41 allowed an attacker who convinced a user to install a malicious extension to leak cross-origin data via a crafted Chrome Extension.
CVE-2022-1489	Out of bounds memory access in UI Shelf in Google Chrome on Chrome OS, Lacros prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via specific user interactions.
CVE-2022-1490	Use after free in Browser Switcher in Google Chrome prior to 101.0.4951.41 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1491	Use after free in Bookmarks in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via specific and direct user interaction.

CVE-2022-1492	Insufficient data validation in Blink Editing in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to inject arbitrary scripts or HTML via a crafted HTML page.
CVE-2022-1493	Use after free in Dev Tools in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via specific and direct user interaction.
CVE-2022-1494	Insufficient data validation in Trusted Types in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to bypass trusted types policy via a crafted HTML page.
CVE-2022-1495	Incorrect security UI in Downloads in Google Chrome on Android prior to 101.0.4951.41 allowed a remote attacker to spoof the APK downloads dialog via a crafted HTML page.
CVE-2022-1496	Use after free in File Manager in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to potentially exploit heap corruption via specific and direct user interaction.
CVE-2022-1497	Inappropriate implementation in Input in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to spoof the contents of cross-origin websites via a crafted HTML page.
CVE-2022-1498	Inappropriate implementation in HTML Parser in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2022-1499	Inappropriate implementation in WebAuthentication in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to bypass same origin policy via a crafted HTML page.
CVE-2022-1500	Insufficient data validation in Dev Tools in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2022-1501	Inappropriate implementation in iframe in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2022-1516	A NULL pointer dereference flaw was found in the Linux kernel's X.25 set of standardized network protocols functionality in the way a user terminates their session using a simulated Ethernet card and continued usage of this connection. This flaw allows a local user to crash the system.
CVE-2022-1616	Use after free in append_command in GitHub repository vim/vim prior to 8.2.4895. This vulnerability is capable

	of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution
CVE-2022-1619	Heap-based Buffer Overflow in function cmdline_erase_chars in GitHub repository vim/vim prior to 8.2.4899. This vulnerabilities are capable of crashing software, modify memory, and possible remote execution
CVE-2022-1620	NULL Pointer Dereference in function vim_regexec_string at regexp.c:2729 in GitHub repository vim/vim prior to 8.2.4901. NULL Pointer Dereference in function vim_regexec_string at regexp.c:2729 allows attackers to cause a denial of service (application crash) via a crafted input.
CVE-2022-1621	Heap buffer overflow in vim_strncpy find_word in GitHub repository vim/vim prior to 8.2.4919. This vulnerability is capable of crashing software, Bypass Protection Mechanism, Modify Memory, and possible remote execution
CVE-2022-1629	Buffer Over-read in function find_next_quote in GitHub repository vim/vim prior to 8.2.4925. This vulnerabilities are capable of crashing software, Modify Memory, and possible remote execution
CVE-2022-1633	Use after free in Sharesheet in Google Chrome on Chrome OS prior to 101.0.4951.64 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via specific user interactions.
CVE-2022-1634	Use after free in Browser UI in Google Chrome prior to 101.0.4951.64 allowed a remote attacker who had convinced a user to engage in specific UI interaction to potentially exploit heap corruption via specific user interactions.
CVE-2022-1635	Use after free in Permission Prompts in Google Chrome prior to 101.0.4951.64 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via specific user interactions.
CVE-2022-1636	Use after free in Performance APIs in Google Chrome prior to 101.0.4951.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1637	Inappropriate implementation in Web Contents in Google Chrome prior to 101.0.4951.64 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2022-1638	Heap buffer overflow in V8 Internationalization in Google Chrome prior to 101.0.4951.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2022-1639	Use after free in ANGLE in Google Chrome prior to 101.0.4951.64 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1640	Use after free in Sharing in Google Chrome prior to 101.0.4951.64 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1641	Use after free in Web UI Diagnostics in Google Chrome on Chrome OS prior to 101.0.4951.64 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via specific user interaction.
CVE-2022-1674	NULL Pointer Dereference in function vim_reexec_string at regexp.c:2733 in GitHub repository vim/vim prior to 8.2.4938. NULL Pointer Dereference in function vim_reexec_string at regexp.c:2733 allows attackers to cause a denial of service (application crash) via a crafted input.
CVE-2022-1720	Buffer Over-read in function grab_file_name in GitHub repository vim/vim prior to 8.2.4956. This vulnerability is capable of crashing the software, memory modification, and possible remote execution.
CVE-2022-1725	NULL Pointer Dereference in GitHub repository vim/vim prior to 8.2.4959.
CVE-2022-1729	A race condition was found the Linux kernel in perf_event_open() which can be exploited by an unprivileged user to gain root privileges. The bug allows to build several exploit primitives such as kernel address information leak, arbitrary execution, etc.
CVE-2022-1733	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.4968.
CVE-2022-1735	Classic Buffer Overflow in GitHub repository vim/vim prior to 8.2.4969.
CVE-2022-1769	Buffer Over-read in GitHub repository vim/vim prior to 8.2.4974.
CVE-2022-1771	Uncontrolled Recursion in GitHub repository vim/vim prior to 8.2.4975.
CVE-2022-1785	Out-of-bounds Write in GitHub repository vim/vim prior to 8.2.4977.
CVE-2022-1786	A use-after-free flaw was found in the Linux kernel's io_uring subsystem in the way a user sets up a ring with IORING_SETUP_IOPOLL with more than one task completing submissions on this ring. This flaw allows a local user to crash or escalate their privileges on the system.
CVE-2022-1789	With shadow paging enabled, the INVPCID instruction results in a call to kvm_mmu_invpcid_gva. If INVPCID

	is executed with CR0.PG=0, the invlpg callback is not set and the result is a NULL pointer dereference.
CVE-2022-1796	Use After Free in GitHub repository vim/vim prior to 8.2.4979.
CVE-2022-1851	Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.
CVE-2022-1852	A NULL pointer dereference flaw was found in the Linux kernel's KVM module, which can lead to a denial of service in the x86_emulate_insn in arch/x86/kvm/emulate.c. This flaw occurs while executing an illegal instruction in guest in the Intel CPU.
CVE-2022-1853	Use after free in Indexed DB in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2022-1854	Use after free in ANGLE in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1855	Use after free in Messaging in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1856	Use after free in User Education in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension or specific user interaction.
CVE-2022-1857	Insufficient policy enforcement in File System API in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to bypass file system restrictions via a crafted HTML page.
CVE-2022-1858	Out of bounds read in DevTools in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to perform an out of bounds memory read via specific user interaction.
CVE-2022-1859	Use after free in Performance Manager in Google Chrome prior to 102.0.5005.61 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1860	Use after free in UI Foundations in Google Chrome on Chrome OS prior to 102.0.5005.61 allowed a remote attacker who convinced a user to engage in specific user interaction to potentially exploit heap corruption via specific user interactions.
CVE-2022-1861	Use after free in Sharing in Google Chrome on Chrome OS prior to 102.0.5005.61 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific user interaction.

CVE-2022-1862	Inappropriate implementation in Extensions in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to bypass profile restrictions via a crafted HTML page.
CVE-2022-1863	Use after free in Tab Groups in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension and specific user interaction.
CVE-2022-1864	Use after free in WebApp Installs in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension and specific user interaction.
CVE-2022-1865	Use after free in Bookmarks in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension and specific user interaction.
CVE-2022-1866	Use after free in Tablet Mode in Google Chrome on Chrome OS prior to 102.0.5005.61 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific user interactions.
CVE-2022-1867	Insufficient validation of untrusted input in Data Transfer in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to bypass same origin policy via a crafted clipboard content.
CVE-2022-1868	Inappropriate implementation in Extensions API in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to bypass navigation restrictions via a crafted HTML page.
CVE-2022-1869	Type Confusion in V8 in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1870	Use after free in App Service in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2022-1871	Insufficient policy enforcement in File System API in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to bypass file system policy via a crafted HTML page.
CVE-2022-1872	Insufficient policy enforcement in Extensions API in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious

	extension to bypass downloads policy via a crafted HTML page.
CVE-2022-1873	Insufficient policy enforcement in COOP in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2022-1874	Insufficient policy enforcement in Safe Browsing in Google Chrome on Mac prior to 102.0.5005.61 allowed a remote attacker to bypass downloads protection policy via a crafted HTML page.
CVE-2022-1875	Inappropriate implementation in PDF in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2022-1876	Heap buffer overflow in DevTools in Google Chrome prior to 102.0.5005.61 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-1886	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.
CVE-2022-1897	Out-of-bounds Write in GitHub repository vim/vim prior to 8.2.
CVE-2022-1898	Use After Free in GitHub repository vim/vim prior to 8.2.
CVE-2022-1927	Buffer Over-read in GitHub repository vim/vim prior to 8.2.
CVE-2022-1942	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.
CVE-2022-1966	A use-after-free vulnerability was found in the Linux kernel's Netfilter subsystem in net/netfilter/nf_tables_api.c. This flaw allows a local attacker with user access to cause a privilege escalation issue.
CVE-2022-1968	Use After Free in GitHub repository vim/vim prior to 8.2.
CVE-2022-1973	A use-after-free flaw was found in the Linux kernel in log_replay in fs/ntfs3/fslog.c in the NTFS journal. This flaw allows a local attacker to crash the system and leads to a kernel information leak problem.
CVE-2022-2000	Out-of-bounds Write in GitHub repository vim/vim prior to 8.2.
CVE-2022-2007	Use after free in WebGPU in Google Chrome prior to 102.0.5005.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2008	Double free in WebGL in Google Chrome prior to 102.0.5005.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2010	Out of bounds read in compositing in Google Chrome prior to 102.0.5005.115 allowed a remote attacker who

	had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2022-2011	Use after free in ANGLE in Google Chrome prior to 102.0.5005.115 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2042	Use After Free in GitHub repository vim/vim prior to 8.2.
CVE-2022-2068	In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 3.0.4 (Affected 3.0.0,3.0.1,3.0.2,3.0.3). Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o). Fixed in OpenSSL 1.0.2zf (Affected 1.0.2-1.0.2ze).
CVE-2022-2078	A vulnerability was found in the Linux kernel's nft_set_desc_concat_parse() function .This flaw allows an attacker to trigger a buffer overflow via nft_set_desc_concat_parse() , causing a denial of service and possibly to run code.
CVE-2022-21151	Processor optimization removal or modification of security-critical code for some Intel(R) Processors may allow an authenticated user to potentially enable information disclosure via local access.
CVE-2022-2124	Buffer Over-read in GitHub repository vim/vim prior to 8.2.
CVE-2022-21248	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the

	internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2022-2125	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.
CVE-2022-2126	Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.
CVE-2022-21271	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2022-21277	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).

	impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2022-21282	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2022-21283	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2022-2129	Out-of-bounds Write in GitHub repository vim/vim prior to 8.2.
CVE-2022-21291	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13,

	<p>17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).</p>
CVE-2022-21293	<p>Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).</p>
CVE-2022-21294	<p>Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. Note: This</p>

	<p>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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).</p>
CVE-2022-21296	<p>Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).</p>
CVE-2022-21299	<p>Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).</p>

	impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2022-21305	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2022-21340	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2022-21341	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Serialization). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows

	unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2022-21349	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: 2D). Supported versions that are affected are Oracle Java SE: 7u321, 8u311; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2022-21360	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2022-21365	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 7u321, 8u311, 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2022-21366	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: ImageIO). Supported versions that are affected are Oracle Java SE: 11.0.13, 17.01; Oracle GraalVM Enterprise Edition: 20.3.4 and 21.3.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).

CVE-2022-21426	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JAXP). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2022-21434	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2022-21443	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE,

	<p>Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Oracle Java SE, Oracle GraalVM Enterprise Edition. 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 can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).</p>
CVE-2022-21449	<p>Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 17.0.2 and 18; Oracle GraalVM Enterprise Edition: 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 7.5 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N).</p>
CVE-2022-21476	<p>Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and</p>

	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 3.1 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2022-21496	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: JNDI). Supported versions that are affected are Oracle Java SE: 7u331, 8u321, 11.0.14, 17.0.2, 18; Oracle GraalVM Enterprise Edition: 20.3.5, 21.3.1 and 22.0.0.2. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2022-21499	KGDB and KDB allow read and write access to kernel memory, and thus should be restricted during lockdown. An attacker with access to a serial port could trigger the debugger so it is important that the debugger respect the lockdown mode when/if it is triggered. CVSS 3.1 Base Score 6.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:U/C:H/I:H/A:H).
CVE-2022-21540	Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2 and 22.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and

	<p>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 3.1 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N).</p>
CVE-2022-21541	<p>Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Hotspot). Supported versions that are affected are Oracle Java SE: 7u343, 8u333, 11.0.15.1, 17.0.3.1, 18.0.1.1; Oracle GraalVM Enterprise Edition: 20.3.6, 21.3.2 and 22.1.0. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.9 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N).</p>
CVE-2022-21549	<p>Vulnerability in the Oracle Java SE, Oracle GraalVM Enterprise Edition product of Oracle Java SE (component: Libraries). Supported versions that are affected are Oracle Java SE: 17.0.3.1; Oracle GraalVM Enterprise Edition: 21.3.2 and 22.1.0. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Oracle Java SE, Oracle GraalVM Enterprise Edition. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Oracle Java SE, Oracle GraalVM Enterprise Edition accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.1 Base Score 5.3 (Integrity impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N).</p>

CVE-2022-2156	Use after free in Core in Google Chrome prior to 103.0.5060.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2157	Use after free in Interest groups in Google Chrome prior to 103.0.5060.53 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2158	Type confusion in V8 in Google Chrome prior to 103.0.5060.53 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2160	Insufficient policy enforcement in DevTools in Google Chrome on Windows prior to 103.0.5060.53 allowed an attacker who convinced a user to install a malicious extension to obtain potentially sensitive information from a user's local files via a crafted HTML page.
CVE-2022-2161	Use after free in WebApp Provider in Google Chrome prior to 103.0.5060.53 allowed a remote attacker who convinced the user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions.
CVE-2022-2162	Insufficient policy enforcement in File System API in Google Chrome on Windows prior to 103.0.5060.53 allowed a remote attacker to bypass file system access via a crafted HTML page.
CVE-2022-2163	Use after free in Cast UI and Toolbar in Google Chrome prior to 103.0.5060.134 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via UI interaction.
CVE-2022-2164	Inappropriate implementation in Extensions API in Google Chrome prior to 103.0.5060.53 allowed an attacker who convinced a user to install a malicious extension to bypass discretionary access control via a crafted HTML page.
CVE-2022-2165	Insufficient data validation in URL formatting in Google Chrome prior to 103.0.5060.53 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2022-21658	Rust is a multi-paradigm, general-purpose programming language designed for performance and safety, especially safe concurrency. The Rust Security Response WG was notified that the `std::fs::remove_dir_all` standard library function is vulnerable a race condition enabling symlink following (CWE-363). An attacker could use this security issue to trick a privileged program into deleting files and directories the attacker couldn't otherwise access or delete. Rust 1.0.0 through Rust 1.58.0 is affected by this vulnerability with 1.58.1 containing a patch. Note that the following build targets don't have usable APIs to properly mitigate the attack, and are thus still

	vulnerable even with a patched toolchain: macOS before version 10.10 (Yosemite) and REDOX. We recommend everyone to update to Rust 1.58.1 as soon as possible, especially people developing programs expected to run in privileged contexts (including system daemons and setuid binaries), as those have the highest risk of being affected by this. Note that adding checks in your codebase before calling remove_dir_all will not mitigate the vulnerability, as they would also be vulnerable to race conditions like remove_dir_all itself. The existing mitigation is working as intended outside of race conditions.
CVE-2022-2175	Buffer Over-read in GitHub repository vim/vim prior to 8.2.
CVE-2022-2182	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.
CVE-2022-2183	Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.
CVE-2022-2206	Out-of-bounds Read in GitHub repository vim/vim prior to 8.2.
CVE-2022-2207	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.
CVE-2022-2208	NULL Pointer Dereference in GitHub repository vim/vim prior to 8.2.5163.
CVE-2022-2210	Out-of-bounds Write in GitHub repository vim/vim prior to 8.2.
CVE-2022-2231	NULL Pointer Dereference in GitHub repository vim/vim prior to 8.2.
CVE-2022-22576	An improper authentication vulnerability exists in curl 7.33.0 to and including 7.82.0 which might allow reuse OAuth2-authenticated connections without properly making sure that the connection was authenticated with the same credentials as set for this transfer. This affects SASL-enabled protocols: SMTP(S), IMAP(S), POP3(S) and LDAP(S) (openldap only).
CVE-2022-22719	A carefully crafted request body can cause a read to a random memory area which could cause the process to crash. This issue affects Apache HTTP Server 2.4.52 and earlier.
CVE-2022-22720	Apache HTTP Server 2.4.52 and earlier fails to close inbound connection when errors are encountered discarding the request body, exposing the server to HTTP Request Smuggling
CVE-2022-22721	If LimitXMLRequestBody is set to allow request bodies larger than 350MB (defaults to 1M) on 32 bit systems an integer overflow happens which later causes out of bounds writes. This issue affects Apache HTTP Server 2.4.52 and earlier.

CVE-2022-22784	The Zoom Client for Meetings (for Android, iOS, Linux, MacOS, and Windows) before version 5.10.0 failed to properly parse XML stanzas in XMPP messages. This can allow a malicious user to break out of the current XMPP message context and create a new message context to have the receiving users client perform a variety of actions. This issue could be used in a more sophisticated attack to forge XMPP messages from the server.
CVE-2022-22785	The Zoom Client for Meetings (for Android, iOS, Linux, MacOS, and Windows) before version 5.10.0 failed to properly constrain client session cookies to Zoom domains. This issue could be used in a more sophisticated attack to send an unsuspecting users Zoom-scoped session cookies to a non-Zoom domain. This could potentially allow for spoofing of a Zoom user.
CVE-2022-22786	The Zoom Client for Meetings for Windows before version 5.10.0 and Zoom Rooms for Conference Room for Windows before version 5.10.0, fails to properly check the installation version during the update process. This issue could be used in a more sophisticated attack to trick a user into downgrading their Zoom client to a less secure version.
CVE-2022-22787	The Zoom Client for Meetings (for Android, iOS, Linux, macOS, and Windows) before version 5.10.0 fails to properly validate the hostname during a server switch request. This issue could be used in a more sophisticated attack to trick an unsuspecting users client to connect to a malicious server when attempting to use Zoom services.
CVE-2022-22815	path_getbbox in path.c in Pillow before 9.0.0 improperly initializes ImagePath.Path.
CVE-2022-22816	path_getbbox in path.c in Pillow before 9.0.0 has a buffer over-read during initialization of ImagePath.Path.
CVE-2022-22817	PIL.ImageMath.eval in Pillow before 9.0.0 allows evaluation of arbitrary expressions, such as ones that use the Python exec method. A lambda expression could also be used,
CVE-2022-22822	addBinding in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-22823	build_model in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-22824	defineAttribute in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-22825	lookup in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-22826	nextScaffoldPart in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.

CVE-2022-22827	storeAttrs in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow.
CVE-2022-22844	LibTIFF 4.3.0 has an out-of-bounds read in _TIFFmemcpy in tif_unix.c in certain situations involving a custom tag and 0x0200 as the second word of the DE field.
CVE-2022-2294	Heap buffer overflow in WebRTC in Google Chrome prior to 103.0.5060.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2295	Type confusion in V8 in Google Chrome prior to 103.0.5060.114 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-22954	VMware Workspace ONE Access and Identity Manager contain a remote code execution vulnerability due to server-side template injection. A malicious actor with network access can trigger a server-side template injection that may result in remote code execution.
CVE-2022-22957	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two remote code execution vulnerabilities (CVE-2022-22957 & CVE-2022-22958). A malicious actor with administrative access can trigger deserialization of untrusted data through malicious JDBC URI which may result in remote code execution.
CVE-2022-22958	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain two remote code execution vulnerabilities (CVE-2022-22957 & CVE-2022-22958). A malicious actor with administrative access can trigger deserialization of untrusted data through malicious JDBC URI which may result in remote code execution.
CVE-2022-22959	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a cross site request forgery vulnerability. A malicious actor can trick a user through a cross site request forgery to unintentionally validate a malicious JDBC URI.
CVE-2022-22960	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain a privilege escalation vulnerability due to improper permissions in support scripts. A malicious actor with local access can escalate privileges to 'root'.
CVE-2022-22961	VMware Workspace ONE Access, Identity Manager and vRealize Automation contain an information disclosure vulnerability due to returning excess information. A malicious actor with remote access may leak the hostname of the target system. Successful exploitation of this issue can lead to targeting victims.

CVE-2022-22965	A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.
CVE-2022-2318	There are use-after-free vulnerabilities caused by timer handler in net/rose/rose_timer.c of linux that allow attackers to crash linux kernel without any privileges.
CVE-2022-23218	The deprecated compatibility function svcunix_create in the sunrpc module of the GNU C Library (aka glibc) through 2.34 copies its path argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.
CVE-2022-23219	The deprecated compatibility function clnt_create in the sunrpc module of the GNU C Library (aka glibc) through 2.34 copies its hostname argument on the stack without validating its length, which may result in a buffer overflow, potentially resulting in a denial of service or (if an application is not built with a stack protector enabled) arbitrary code execution.
CVE-2022-23222	kernel/bpf/verifier.c in the Linux kernel through 5.15.14 allows local users to gain privileges because of the availability of pointer arithmetic via certain *_OR_NULL pointer types.
CVE-2022-23302	JMSSink in all versions of Log4j 1.x is vulnerable to deserialization of untrusted data when the attacker has write access to the Log4j configuration or if the configuration references an LDAP service the attacker has access to. The attacker can provide a TopicConnectionFactoryBindingName configuration causing JMSSink to perform JNDI requests that result in remote code execution in a similar fashion to CVE-2021-4104. Note this issue only affects Log4j 1.x when specifically configured to use JMSSink, which is not the default. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.
CVE-2022-23305	By design, the JDBCAppender in Log4j 1.2.x accepts an SQL statement as a configuration parameter where the values to be inserted are converters from PatternLayout. The message converter, %m, is likely to always be included. This allows attackers to manipulate the SQL by entering crafted strings into input fields or headers of an application that are logged allowing unintended SQL queries to be executed. Note this

	issue only affects Log4j 1.x when specifically configured to use the JDBCAppender, which is not the default. Beginning in version 2.0-beta8, the JDBCAppender was re-introduced with proper support for parameterized SQL queries and further customization over the columns written to in logs. Apache Log4j 1.2 reached end of life in August 2015. Users should upgrade to Log4j 2 as it addresses numerous other issues from the previous versions.
CVE-2022-23307	CVE-2020-9493 identified a deserialization issue that was present in Apache Chainsaw. Prior to Chainsaw V2.0 Chainsaw was a component of Apache Log4j 1.2.x where the same issue exists.
CVE-2022-23308	valid.c in libxml2 before 2.9.13 has a use-after-free of ID and IDREF attributes.
CVE-2022-23648	containerd is a container runtime available as a daemon for Linux and Windows. A bug was found in containerd prior to versions 1.6.1, 1.5.10, and 1.14.12 where containers launched through containerd's CRI implementation on Linux with a specially-crafted image configuration could gain access to read-only copies of arbitrary files and directories on the host. This may bypass any policy-based enforcement on container setup (including a Kubernetes Pod Security Policy) and expose potentially sensitive information. Kubernetes and crictl can both be configured to use containerd's CRI implementation. This bug has been fixed in containerd 1.6.1, 1.5.10, and 1.4.12. Users should update to these versions to resolve the issue.
CVE-2022-23772	Rat.SetString in math/big in Go before 1.16.14 and 1.17.x before 1.17.7 has an overflow that can lead to Uncontrolled Memory Consumption.
CVE-2022-23773	cmd/go in Go before 1.16.14 and 1.17.x before 1.17.7 can misinterpret branch names that falsely appear to be version tags. This can lead to incorrect access control if an actor is supposed to be able to create branches but not tags.
CVE-2022-23806	Curve.IsOnCurve in crypto/elliptic in Go before 1.16.14 and 1.17.x before 1.17.7 can incorrectly return true in situations with a big.Int value that is not a valid field element.
CVE-2022-23852	Expat (aka libexpat) before 2.4.4 has a signed integer overflow in XML_GetBuffer, for configurations with a nonzero XML_CONTEXT_BYTES.
CVE-2022-23943	Out-of-bounds Write vulnerability in mod_sed of Apache HTTP Server allows an attacker to overwrite heap memory with possibly attacker provided data. This issue affects Apache HTTP Server 2.4 version 2.4.52 and prior versions.

CVE-2022-23960	Certain Arm Cortex and Neoverse processors through 2022-03-08 do not properly restrict cache speculation, aka Spectre-BHB. An attacker can leverage the shared branch history in the Branch History Buffer (BHB) to influence mispredicted branches. Then, cache allocation can allow the attacker to obtain sensitive information.
CVE-2022-24407	In Cyrus SASL 2.1.17 through 2.1.27 before 2.1.28, plugins/sql.c does not escape the password for a SQL INSERT or UPDATE statement.
CVE-2022-24448	An issue was discovered in fs/nfs/dir.c in the Linux kernel before 5.16.5. If an application sets the O_DIRECTORY flag, and tries to open a regular file, nfs_atomic_open() performs a regular lookup. If a regular file is found, ENOTDIR should occur, but the server instead returns uninitialized data in the file descriptor.
CVE-2022-24675	encoding/pem in Go before 1.17.9 and 1.18.x before 1.18.1 has a Decode stack overflow via a large amount of PEM data.
CVE-2022-24713	regex is an implementation of regular expressions for the Rust language. The regex crate features built-in mitigations to prevent denial of service attacks caused by untrusted regexes, or untrusted input matched by trusted regexes. Those (tunable) mitigations already provide sane defaults to prevent attacks. This guarantee is documented and it's considered part of the crate's API. Unfortunately a bug was discovered in the mitigations designed to prevent untrusted regexes to take an arbitrary amount of time during parsing, and it's possible to craft regexes that bypass such mitigations. This makes it possible to perform denial of service attacks by sending specially crafted regexes to services accepting user-controlled, untrusted regexes. All versions of the regex crate before or equal to 1.5.4 are affected by this issue. The fix is include starting from regex 1.5.5. All users accepting user-controlled regexes are recommended to upgrade immediately to the latest version of the regex crate. Unfortunately there is no fixed set of problematic regexes, as there are practically infinite regexes that could be crafted to exploit this vulnerability. Because of this, it us not recommend to deny known problematic regexes.
CVE-2022-24765	Git for Windows is a fork of Git containing Windows-specific patches. This vulnerability affects users working on multi-user machines, where untrusted parties have write access to the same hard disk. Those untrusted parties could create the folder 'C:\.git', which would be picked up by Git operations run supposedly outside a repository while searching for a Git directory. Git would then respect any config in said Git directory. Git Bash

	<p>users who set `GIT_PS1_SHOWDIRTYSTATE` are vulnerable as well. Users who installed posh-git are vulnerable simply by starting a PowerShell. Users of IDEs such as Visual Studio are vulnerable: simply creating a new project would already read and respect the config specified in `C:\.git\config`. Users of the Microsoft fork of Git are vulnerable simply by starting a Git Bash. The problem has been patched in Git for Windows v2.35.2. Users unable to upgrade may create the folder `.git` on all drives where Git commands are run, and remove read/write access from those folders as a workaround. Alternatively, define or extend `GIT_CEILING_DIRECTORIES` to cover the _parent_directory of the user profile, e.g. `C:\Users` if the user profile is located in `C:\Users\my-user-name`.</p>
CVE-2022-24769	<p>Moby is an open-source project created by Docker to enable and accelerate software containerization. A bug was found in Moby (Docker Engine) prior to version 20.10.14 where containers were incorrectly started with non-empty inheritable Linux process capabilities, creating an atypical Linux environment and enabling programs with inheritable file capabilities to elevate those capabilities to the permitted set during `execve(2)`. Normally, when executable programs have specified permitted file capabilities, otherwise unprivileged users and processes can execute those programs and gain the specified file capabilities up to the bounding set. Due to this bug, containers which included executable programs with inheritable file capabilities allowed otherwise unprivileged users and processes to additionally gain these inheritable file capabilities up to the container's bounding set. Containers which use Linux users and groups to perform privilege separation inside the container are most directly impacted. This bug did not affect the container security sandbox as the inheritable set never contained more capabilities than were included in the container's bounding set. This bug has been fixed in Moby (Docker Engine) 20.10.14. Running containers should be stopped, deleted, and recreated for the inheritable capabilities to be reset. This fix changes Moby (Docker Engine) behavior such that containers are started with a more typical Linux environment. As a workaround, the entry point of a container can be modified to use a utility like `capsh(1)` to drop inheritable capabilities prior to the primary process starting.</p>
CVE-2022-2477	<p>Use after free in Guest View in Google Chrome prior to 103.0.5060.134 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.</p>

CVE-2022-2478	Use after free in PDF in Google Chrome prior to 103.0.5060.134 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2479	Insufficient validation of untrusted input in File in Google Chrome on Android prior to 103.0.5060.134 allowed an attacker who convinced a user to install a malicious app to obtain potentially sensitive information from internal file directories via a crafted HTML page.
CVE-2022-2480	Use after free in Service Worker API in Google Chrome prior to 103.0.5060.134 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-24801	Twisted is an event-based framework for internet applications, supporting Python 3.6+. Prior to version 22.4.0rc1, the Twisted Web HTTP 1.1 server, located in the `twisted.web.http` module, parsed several HTTP request constructs more leniently than permitted by RFC 7230. This non-conformant parsing can lead to desync if requests pass through multiple HTTP parsers, potentially resulting in HTTP request smuggling. Users who may be affected use Twisted Web's HTTP 1.1 server and/or proxy and also pass requests through a different HTTP server and/or proxy. The Twisted Web client is not affected. The HTTP 2.0 server uses a different parser, so it is not affected. The issue has been addressed in Twisted 22.4.0rc1. Two workarounds are available: Ensure any vulnerabilities in upstream proxies have been addressed, such as by upgrading them; or filter malformed requests by other means, such as configuration of an upstream proxy.
CVE-2022-2481	Use after free in Views in Google Chrome prior to 103.0.5060.134 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via UI interaction.
CVE-2022-24903	Rsyslog is a rocket-fast system for log processing. Modules for TCP syslog reception have a potential heap buffer overflow when octet-counted framing is used. This can result in a segfault or some other malfunction. As of our understanding, this vulnerability can not be used for remote code execution. But there may still be a slight chance for experts to do that. The bug occurs when the octet count is read. While there is a check for the maximum number of octets, digits are written to a heap buffer even when the octet count is over the maximum. This can be used to overrun the memory buffer. However, once the sequence of digits stop, no additional characters can be added to the buffer. In our opinion, this makes remote exploits impossible or at least highly complex. Octet-counted framing is one of two potential framing modes. It is relatively uncommon, but enabled by default on

	receivers. Modules `imtcp`, `imptcp`, `imgssapi`, and `imhttp` are used for regular syslog message reception. It is best practice not to directly expose them to the public. When this practice is followed, the risk is considerably lower. Module `imdiag` is a diagnostics module primarily intended for testbench runs. We do not expect it to be present on any production installation. Octet-counted framing is not very common. Usually, it needs to be specifically enabled at senders. If users do not need it, they can turn it off for the most important modules. This will mitigate the vulnerability.
CVE-2022-24921	regexp.Compile in Go before 1.16.15 and 1.17.x before 1.17.8 allows stack exhaustion via a deeply nested expression.
CVE-2022-25235	xmltok_impl.c in Expat (aka libexpat) before 2.4.5 lacks certain validation of encoding, such as checks for whether a UTF-8 character is valid in a certain context.
CVE-2022-25236	xmlparse.c in Expat (aka libexpat) before 2.4.5 allows attackers to insert namespace-separator characters into namespace URIs.
CVE-2022-25315	In Expat (aka libexpat) before 2.4.5, there is an integer overflow in storeRawNames.
CVE-2022-25636	net/netfilter/nf_dup_netdev.c in the Linux kernel 5.4 through 5.6.10 allows local users to gain privileges because of a heap out-of-bounds write. This is related to nf_tables_offload.
CVE-2022-2603	Use after free in Omnibox in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2604	Use after free in Safe Browsing in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2605	Out of bounds read in Dawn in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2606	Use after free in Managed devices API in Google Chrome prior to 104.0.5112.79 allowed a remote attacker who convinced a user to enable a specific Enterprise policy to potentially exploit heap corruption via a crafted HTML page.
CVE-2022-2607	Use after free in Tab Strip in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions.
CVE-2022-2608	Use after free in Overview Mode in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific

	user interactions to potentially exploit heap corruption via specific UI interactions.
CVE-2022-2609	Use after free in Nearby Share in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions.
CVE-2022-2610	Insufficient policy enforcement in Background Fetch in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2022-2611	Inappropriate implementation in Fullscreen API in Google Chrome on Android prior to 104.0.5112.79 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2022-2612	Side-channel information leakage in Keyboard input in Google Chrome prior to 104.0.5112.79 allowed a remote attacker who had compromised the renderer process to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2022-2613	Use after free in Input in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions.
CVE-2022-26134	In affected versions of Confluence Server and Data Center, an OGNL injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. The affected versions are from 1.3.0 before 7.4.17, from 7.13.0 before 7.13.7, from 7.14.0 before 7.14.3, from 7.15.0 before 7.15.2, from 7.16.0 before 7.16.4, from 7.17.0 before 7.17.4, and from 7.18.0 before 7.18.1.
CVE-2022-26136	A vulnerability in multiple Atlassian products allows a remote, unauthenticated attacker to bypass Servlet Filters used by first and third party apps. The impact depends on which filters are used by each app, and how the filters are used. This vulnerability can result in authentication bypass and cross-site scripting. Atlassian has released updates that fix the root cause of this vulnerability, but has not exhaustively enumerated all potential consequences of this vulnerability. Atlassian Bamboo versions are affected before 8.0.9, from 8.1.0 before 8.1.8, and from 8.2.0 before 8.2.4. Atlassian Bitbucket versions are affected before 7.6.16, from 7.7.0 before 7.17.8, from 7.18.0 before 7.19.5, from 7.20.0 before 7.20.2, from 7.21.0 before 7.21.2, and versions 8.0.0 and 8.1.0. Atlassian Confluence versions are affected before 7.4.17, from 7.5.0 before 7.13.7, from 7.14.0 before 7.14.3, from 7.15.0 before 7.15.2,

	from 7.16.0 before 7.16.4, from 7.17.0 before 7.17.4, and version 7.21.0. Atlassian Crowd versions are affected before 4.3.8, from 4.4.0 before 4.4.2, and version 5.0.0. Atlassian Fisheye and Crucible versions before 4.8.10 are affected. Atlassian Jira versions are affected before 8.13.22, from 8.14.0 before 8.20.10, and from 8.21.0 before 8.22.4. Atlassian Jira Service Management versions are affected before 4.13.22, from 4.14.0 before 4.20.10, and from 4.21.0 before 4.22.4.
CVE-2022-26137	A vulnerability in multiple Atlassian products allows a remote, unauthenticated attacker to cause additional Servlet Filters to be invoked when the application processes requests or responses. Atlassian has confirmed and fixed the only known security issue associated with this vulnerability: Cross-origin resource sharing (CORS) bypass. Sending a specially crafted HTTP request can invoke the Servlet Filter used to respond to CORS requests, resulting in a CORS bypass. An attacker that can trick a user into requesting a malicious URL can access the vulnerable application with the victim's permissions. Atlassian Bamboo versions are affected before 8.0.9, from 8.1.0 before 8.1.8, and from 8.2.0 before 8.2.4. Atlassian Bitbucket versions are affected before 7.6.16, from 7.7.0 before 7.17.8, from 7.18.0 before 7.19.5, from 7.20.0 before 7.20.2, from 7.21.0 before 7.21.2, and versions 8.0.0 and 8.1.0. Atlassian Confluence versions are affected before 7.4.17, from 7.5.0 before 7.13.7, from 7.14.0 before 7.14.3, from 7.15.0 before 7.15.2, from 7.16.0 before 7.16.4, from 7.17.0 before 7.17.4, and version 7.21.0. Atlassian Crowd versions are affected before 4.3.8, from 4.4.0 before 4.4.2, and version 5.0.0. Atlassian Fisheye and Crucible versions before 4.8.10 are affected. Atlassian Jira versions are affected before 8.13.22, from 8.14.0 before 8.20.10, and from 8.21.0 before 8.22.4. Atlassian Jira Service Management versions are affected before 4.13.22, from 4.14.0 before 4.20.10, and from 4.21.0 before 4.22.4.
CVE-2022-26138	The Atlassian Questions For Confluence app for Confluence Server and Data Center creates a Confluence user account in the confluence-users group with the username disabledsystemuser and a hardcoded password. A remote, unauthenticated attacker with knowledge of the hardcoded password could exploit this to log into Confluence and access all content accessible to users in the confluence-users group. This user account is created when installing versions 2.7.34, 2.7.35, and 3.0.2 of the app.
CVE-2022-2614	Use after free in Sign-In Flow in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2022-2615	Insufficient policy enforcement in Cookies in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2022-2616	Inappropriate implementation in Extensions API in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to install a malicious extension to spoof the contents of the Omnibox (URL bar) via a crafted Chrome Extension.
CVE-2022-2617	Use after free in Extensions API in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific UI interactions.
CVE-2022-2618	Insufficient validation of untrusted input in Internals in Google Chrome prior to 104.0.5112.79 allowed a remote attacker to bypass download restrictions via a malicious file .
CVE-2022-2619	Insufficient validation of untrusted input in Settings in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to install a malicious extension to inject scripts or HTML into a privileged page via a crafted HTML page.
CVE-2022-2620	Use after free in WebUI in Google Chrome on Chrome OS prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions.
CVE-2022-2621	Use after free in Extensions in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via specific UI interactions.
CVE-2022-2622	Insufficient validation of untrusted input in Safe Browsing in Google Chrome on Windows prior to 104.0.5112.79 allowed a remote attacker to bypass download restrictions via a crafted file.
CVE-2022-2623	Use after free in Offline in Google Chrome on Android prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via specific UI interactions.
CVE-2022-2624	Heap buffer overflow in PDF in Google Chrome prior to 104.0.5112.79 allowed a remote attacker who convinced a user to engage in specific user interactions to potentially exploit heap corruption via a crafted PDF file.
CVE-2022-26365	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond

	to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742).
CVE-2022-26377	Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') vulnerability in mod_proxy_ajp of Apache HTTP Server allows an attacker to smuggle requests to the AJP server it forwards requests to. This issue affects Apache HTTP Server Apache HTTP Server 2.4 version 2.4.53 and prior versions.
CVE-2022-26490	st21nfca_connectivity_event_received in drivers/nfc/st21nfca/se.c in the Linux kernel through 5.16.12 has EVT_TRANSACTION buffer overflows because of untrusted length parameters.
CVE-2022-27666	A heap buffer overflow flaw was found in IPsec ESP transformation code in net/ipv4/esp4.c and net/ipv6/esp6.c. This flaw allows a local attacker with a normal user privilege to overwrite kernel heap objects and may cause a local privilege escalation threat.
CVE-2022-27774	An insufficiently protected credentials vulnerability exists in curl 4.9 to and include curl 7.82.0 are affected that could allow an attacker to extract credentials when follows HTTP(S) redirects is used with authentication could leak credentials to other services that exist on different protocols or port numbers.
CVE-2022-27775	An information disclosure vulnerability exists in curl 7.65.0 to 7.82.0 are vulnerable that by using an IPv6 address that was in the connection pool but with a different zone id it could reuse a connection instead.
CVE-2022-27776	A insufficiently protected credentials vulnerability in fixed in curl 7.83.0 might leak authentication or cookie header data on HTTP redirects to the same host but another port number.
CVE-2022-27782	libcurl would reuse a previously created connection even when a TLS or SSHrelated option had been changed that should have prohibited reuse.libcurl keeps previously used connections in a connection pool for subsequenttransfers to reuse if one of them matches the setup. However, several TLS andSSH settings were left out from the configuration match checks, making themmatch too easily.
CVE-2022-28327	The generic P-256 feature in crypto/elliptic in Go before 1.17.9 and 1.18.x before 1.18.1 allows a panic via long scalar input.

CVE-2022-28330	Apache HTTP Server 2.4.53 and earlier on Windows may read beyond bounds when configured to process requests with the mod_isapi module.
CVE-2022-28356	In the Linux kernel before 5.17.1, a refcount leak bug was found in net/llc/af_llc.c.
CVE-2022-28389	mcba_usb_start_xmit in drivers/net/can/usb/mcba_usb.c in the Linux kernel through 5.17.1 has a double free.
CVE-2022-28390	ems_usb_start_xmit in drivers/net/can/usb/ems_usb.c in the Linux kernel through 5.17.1 has a double free.
CVE-2022-28614	The ap_rwrite() function in Apache HTTP Server 2.4.53 and earlier may read unintended memory if an attacker can cause the server to reflect very large input using ap_rwrite() or ap_rputs(), such as with mod_luas r:puts() function. Modules compiled and distributed separately from Apache HTTP Server that use the 'ap_rputs' function and may pass it a very large (INT_MAX or larger) string must be compiled against current headers to resolve the issue.
CVE-2022-28615	Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.
CVE-2022-28755	The Zoom Client for Meetings (for Android, iOS, Linux, macOS, and Windows) before version 5.11.0 are susceptible to a URL parsing vulnerability. If a malicious Zoom meeting URL is opened, the malicious link may direct the user to connect to an arbitrary network address, leading to additional attacks including the potential for remote code execution through launching executables from arbitrary paths.
CVE-2022-28893	The SUNRPC subsystem in the Linux kernel through 5.17.2 can call xs_xprt_free before ensuring that sockets are in the intended state.
CVE-2022-29149	Azure Open Management Infrastructure (OMI) Elevation of Privilege Vulnerability.
CVE-2022-29155	In OpenLDAP 2.x before 2.5.12 and 2.6.x before 2.6.2, a SQL injection vulnerability exists in the experimental back-sql backend to slapd, via a SQL statement within an LDAP query. This can occur during an LDAP search operation when the search filter is processed, due to a lack of proper escaping.
CVE-2022-29187	Git is a distributed revision control system. Git prior to versions 2.37.1, 2.36.2, 2.35.4, 2.34.4, 2.33.4, 2.32.3, 2.31.4, and 2.30.5, is vulnerable to privilege escalation in all platforms. An unsuspecting user could still be

	affected by the issue reported in CVE-2022-24765, for example when navigating as root into a shared tmp directory that is owned by them, but where an attacker could create a git repository. Versions 2.37.1, 2.36.2, 2.35.4, 2.34.4, 2.33.4, 2.32.3, 2.31.4, and 2.30.5 contain a patch for this issue. The simplest way to avoid being affected by the exploit described in the example is to avoid running git as root (or an Administrator in Windows), and if needed to reduce its use to a minimum. While a generic workaround is not possible, a system could be hardened from the exploit described in the example by removing any such repository if it exists already and creating one as root to block any future attacks.
CVE-2022-29404	In Apache HTTP Server 2.4.53 and earlier, a malicious request to a lua script that calls r:parsebody(0) may cause a denial of service due to no default limit on possible input size.
CVE-2022-29581	Improper Update of Reference Count vulnerability in net/sched of Linux Kernel allows local attacker to cause privilege escalation to root. This issue affects: Linux Kernel versions prior to 5.18; version 4.14 and later versions.
CVE-2022-29582	In the Linux kernel before 5.17.3, fs/io_uring.c has a use-after-free due to a race condition in io_uring timeouts. This can be triggered by a local user who has no access to any user namespace; however, the race condition perhaps can only be exploited infrequently.
CVE-2022-29599	In Apache Maven maven-shared-utils prior to version 3.3.3, the Commandline class can emit double-quoted strings without proper escaping, allowing shell injection attacks.
CVE-2022-30522	If Apache HTTP Server 2.4.53 is configured to do transformations with mod_sed in contexts where the input to mod_sed may be very large, mod_sed may make excessively large memory allocations and trigger an abort.
CVE-2022-30556	Apache HTTP Server 2.4.53 and earlier may return lengths to applications calling r:wsread() that point past the end of the storage allocated for the buffer.
CVE-2022-30594	The Linux kernel before 5.17.2 mishandles seccomp permissions. The PTRACE_SEIZE code path allows attackers to bypass intended restrictions on setting the PT_SUSPEND_SECCOMP flag.
CVE-2022-31030	containerd is an open source container runtime. A bug was found in the containerd's CRI implementation where programs inside a container can cause the containerd daemon to consume memory without bound during invocation of the `ExecSync` API. This can cause containerd to consume all available

	memory on the computer, denying service to other legitimate workloads. Kubernetes and crictl can both be configured to use containerd's CRI implementation; `ExecSync` may be used when running probes or when executing processes via an "exec" facility. This bug has been fixed in containerd 1.6.6 and 1.5.13. Users should update to these versions to resolve the issue. Users unable to upgrade should ensure that only trusted images and commands are used.
CVE-2022-31813	Apache HTTP Server 2.4.53 and earlier may not send the X-Forwarded-* headers to the origin server based on client side Connection header hop-by-hop mechanism. This may be used to bypass IP based authentication on the origin server/application.
CVE-2022-32250	net/netfilter/nf_tables_api.c in the Linux kernel through 5.18.1 allows a local user (able to create user/net namespaces) to escalate privileges to root because an incorrect NFT_STATEFUL_EXPR check leads to a use-after-free.
CVE-2022-32296	The Linux kernel before 5.17.9 allows TCP servers to identify clients by observing what source ports are used.
CVE-2022-32981	An issue was discovered in the Linux kernel through 5.18.3 on powerpc 32-bit platforms. There is a buffer overflow in ptrace PEEKUSER and POKEUSER (aka PEEKUSR and POKEUSR) when accessing floating point registers.
CVE-2022-33640	System Center Operations Manager: Open Management Infrastructure (OMI) Elevation of Privilege Vulnerability.
CVE-2022-33740	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742).
CVE-2022-33741	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page

	as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742).
CVE-2022-33742	Linux disk/nic frontends data leaks T[his CNA information record relates to multiple CVEs; the text explains which aspects/vulnerabilities correspond to which CVE.] Linux Block and Network PV device frontends don't zero memory regions before sharing them with the backend (CVE-2022-26365, CVE-2022-33740). Additionally the granularity of the grant table doesn't allow sharing less than a 4K page, leading to unrelated data residing in the same 4K page as data shared with a backend being accessible by such backend (CVE-2022-33741, CVE-2022-33742).
CVE-2022-33743	network backend may cause Linux netfront to use freed SKBs While adding logic to support XDP (eXpress Data Path), a code label was moved in a way allowing for SKBs having references (pointers) retained for further processing to nevertheless be freed.
CVE-2022-33744	Arm guests can cause Dom0 DoS via PV devices When mapping pages of guests on Arm, dom0 is using an rbtree to keep track of the foreign mappings. Updating of that rbtree is not always done completely with the related lock held, resulting in a small race window, which can be used by unprivileged guests via PV devices to cause inconsistencies of the rbtree. These inconsistencies can lead to Denial of Service (DoS) of dom0, e.g. by causing crashes or the inability to perform further mappings of other guests' memory pages.
CVE-2022-34169	The Apache Xalan Java XSLT library is vulnerable to an integer truncation issue when processing malicious XSLT stylesheets. This can be used to corrupt Java class files generated by the internal XSLTC compiler and execute arbitrary Java bytecode. The Apache Xalan Java project is dormant and in the process of being retired. No future releases of Apache Xalan Java to address this issue are expected. Note: Java runtimes (such as OpenJDK) include repackaged copies of Xalan.
CVE-2022-34266	The libtiff-4.0.3-35.amzn2.0.1 package for LibTIFF on Amazon Linux 2 allows attackers to cause a denial of service (application crash), a different vulnerability than CVE-2022-0562. When processing a malicious TIFF file, an invalid range may be passed as an argument to the memset() function within TIFFFetchStripThing() in tif_dirread.c. This will cause TIFFFetchStripThing() to segfault after use of an uninitialized resource.
CVE-2022-34494	rpmsg_virtio_add_ctrl_dev in drivers/rpmsg/virtio_rpmsg_bus.c in the Linux kernel before 5.18.4 has a double free.

CVE-2022-34495	rpmsg_probe in drivers/rpmsg/virtio_rpmsg_bus.c in the Linux kernel before 5.18.4 has a double free.
CVE-2022-34918	An issue was discovered in the Linux kernel through 5.18.9. A type confusion bug in nft_set_elem_init (leading to a buffer overflow) could be used by a local attacker to escalate privileges, a different vulnerability than CVE-2022-32250. (The attacker can obtain root access, but must start with an unprivileged user namespace to obtain CAP_NET_ADMIN access.) This can be fixed in nft_setelem_parse_data in net/netfilter/nf_tables_api.c.

5.3 Passed rules - Network Reachability-1.1

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

5.4 Passed rules - Security Best Practices-1.0

Rule	Description
Configure Password Complexity	This rule helps determine whether a password complexity mechanism is configured on your EC2 instances.
Configure Password Maximum Age	This rule helps determine whether maximum age for passwords is configured on your EC2 instances.
Configure Password Minimum Length	This rule helps determine whether minimum length for passwords is configured on your EC2 instances.
Configure permissions for system directories	This rule checks permissions on system directories that contain binaries and system configuration information to make sure that only the root user (a user who logs in by using root account credentials) has write permissions for these directories.

Disable Password Authentication Over SSH	This rule helps determine whether your EC2 instances are configured to support password authentication over the SSH protocol.
Disable root login over SSH with a command authenticated by public key	This rule helps determine whether the SSH daemon is configured to permit logging in to your EC2 instance as root using a command authenticated by a public key.
Enable ASLR	This rule helps determine whether address space layout randomization (ASLR) is enabled on the operating systems of the EC2 instances in your assessment target.
Enable DEP	This rule helps determine whether Data Execution Prevention (DEP) is enabled on the operating systems of the EC2 instances in your assessment target.
Support SSH Version 2 Only	This rule helps determine whether your EC2 instances are configured to support SSH protocol version 1.0.