Amazon Inspector - Assessment Report

Full Report

Report generated on 2019-02-12 at 22:01:40 UTC

Assessment Template: Prod-Assessment

Assessment Run start: 2019-02-12 at 20:42:54 UTC
Assessment Run end: 2019-02-12 at 21:44:33 UTC

Section 1: Executive Summary

This is an Inspector assessment report for an assessment started on 2019-02-12 20:42:54 UTC for assessment template 'Prod-Assessment'. The assessment target included 1 instances, and was tested against 5 Rules Packages.

The assessment target is defined using the following EC2 tags

Key	Value
Enviornment	NCS-PROD

The following Rules Packages were assessed. A total of 118 findings were created, with the following distribution by severity:

Rules Package	High	Medium	Low	Informational
CIS Operating System Security Configuration Benchmarks-1.0	77	0	0	9
Common Vulnerabilities and Exposures-1.1	13	12	0	0
Network Reachability-1.1	0	0	0	4
Runtime Behavior Analysis-1.0	0	0	0	2
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: 5

2.1.1: CIS Operating System Security Configuration Benchmarks-1.0

Description: The CIS Security Benchmarks program provides well-defined, un-biased 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 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)
- 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: Runtime Behavior Analysis-1.0

Description: These rules analyze the behavior of your instances during an assessment run, and provide guidance on how to make your instances more secure.
Provider: Amazon Web Services, Inc.
Version: 1.0

2.1.5: 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 - Prod-Assessment

2.2.1: EC2 Tags:

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

Key	Value
Enviornment	NCS-PROD

2.2.2: Instances - Count 1

Instance ID

i-0f30edc8c6bf5cb5a

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 - Server

Rule	Severity	Failed
1.1.16 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 freevxfs filesystems is disabled	High	1
1.1.1.3 Ensure mounting of jffs2 filesystems is disabled	High	1
1.1.1.4 Ensure mounting of hfs filesystems is disabled	High	1
1.1.1.5 Ensure mounting of hfsplus filesystems is disabled	High	1
1.1.1.6 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
1.4.1 Ensure permissions on bootloader config are configured	High	1
1.4.2 Ensure bootloader password is set	High	1
1.5.1 Ensure core dumps are restricted	High	1
1.7.1.4 Ensure permissions on /etc/motd are configured	Informational	1
2.3.4 Ensure telnet client is not installed	High	1
3.1.2 Ensure packet redirect sending is disabled	High	1
3.2.3 Ensure secure ICMP redirects are not accepted	High	1
3.2.4 Ensure suspicious packets are logged	High	1
3.2.8 Ensure TCP SYN Cookies is enabled	High	1
3.3.1 Ensure IPv6 router advertisements are not accepted	Informational	1
3.3.3 Ensure IPv6 is disabled	Informational	1
3.4.3 Ensure /etc/hosts.deny is configured	High	1
3.5.1 Ensure DCCP is disabled	Informational	1

3.5.2 Ensure SCTP is disabled	Informational	1
3.5.3 Ensure RDS is disabled	Informational	1
3.5.4 Ensure TIPC is disabled	Informational	1
3.6.2 Ensure default deny firewall policy	High	1
3.6.3 Ensure loopback traffic is configured	High	1
3.6.5 Ensure firewall rules exist for all open ports	High	1
4.2.4 Ensure permissions on all logfiles are 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
5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured	High	1
5.2.4 Ensure SSH X11 forwarding is disabled	High	1
5.2.5 Ensure SSH MaxAuthTries is set to 4 or less	High	1
5.2.8 Ensure SSH root login is disabled	High	1
5.2.10 Ensure SSH PermitUserEnvironment is disabled	High	1
5.2.11 Ensure only approved MAC algorithms are used	High	1
5.2.12 Ensure SSH Idle Timeout Interval is configured	High	1
5.2.13 Ensure SSH LoginGraceTime is set to one minute or less	High	1
5.2.14 Ensure SSH access is limited	High	1
5.2.15 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	Informational	1
5.3.3 Ensure password reuse is limited	High	1
5.4.2 Ensure system accounts are non-login	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 90 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
6.1.11 Ensure no unowned files or directories exist	High	1
6.1.12 Ensure no ungrouped files or directories exist	High	1
6.2.7 Ensure all users' home directories exist	High	1

6.2.8 Ensure users' home directories permissions are 750 or more restrictive	High	1

3.1.2 Level 1 - Workstation

Rule	Severity	Failed
1.1.16 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 freevxfs filesystems is disabled	High	1
1.1.1.3 Ensure mounting of jffs2 filesystems is disabled	High	1
1.1.1.4 Ensure mounting of hfs filesystems is disabled	High	1
1.1.1.5 Ensure mounting of hfsplus filesystems is disabled	High	1
1.1.1.6 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
1.4.1 Ensure permissions on bootloader config are configured	High	1
1.4.2 Ensure bootloader password is set	High	1
1.5.1 Ensure core dumps are restricted	High	1
1.7.1.4 Ensure permissions on /etc/motd are configured	Informational	1
2.3.4 Ensure telnet client is not installed	High	1
3.1.2 Ensure packet redirect sending is disabled	High	1
3.2.3 Ensure secure ICMP redirects are not accepted	High	1
3.2.4 Ensure suspicious packets are logged	High	1
3.2.8 Ensure TCP SYN Cookies is enabled	High	1
3.3.1 Ensure IPv6 router advertisements are not accepted	Informational	1
3.3.3 Ensure IPv6 is disabled	Informational	1
3.4.3 Ensure /etc/hosts.deny is configured	High	1
3.5.1 Ensure DCCP is disabled	Informational	1
3.5.2 Ensure SCTP is disabled	Informational	1
3.5.3 Ensure RDS is disabled	Informational	1
3.5.4 Ensure TIPC is disabled	Informational	1
3.6.2 Ensure default deny firewall policy	High	1
3.6.3 Ensure loopback traffic is configured	High	1
3.6.5 Ensure firewall rules exist for all open ports	High	1
4.2.4 Ensure permissions on all logfiles are 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
5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured	High	1
5.2.4 Ensure SSH X11 forwarding is disabled	High	1
5.2.5 Ensure SSH MaxAuthTries is set to 4 or less	High	1
5.2.8 Ensure SSH root login is disabled	High	1
5.2.10 Ensure SSH PermitUserEnvironment is disabled	High	1
5.2.11 Ensure only approved MAC algorithms are used	High	1
5.2.12 Ensure SSH Idle Timeout Interval is configured	High	1
5.2.13 Ensure SSH LoginGraceTime is set to one minute or less	High	1
5.2.14 Ensure SSH access is limited	High	1
5.2.15 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	Informational	1
5.3.3 Ensure password reuse is limited	High	1
5.4.2 Ensure system accounts are non-login	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 90 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
6.1.11 Ensure no unowned files or directories exist	High	1
6.1.12 Ensure no ungrouped files or directories exist	High	1
6.2.7 Ensure all users' home directories exist	High	1
6.2.8 Ensure users' home directories permissions are 750 or more restrictive	High	1

3.1.3 Level 2 - Server

Rule	Severity	Failed
1.1.2 Ensure separate partition exists for /tmp	High	1
1.1.5 Ensure separate partition exists for /var	High	1
1.1.6 Ensure separate partition exists for /var/tmp	High	1
1.1.10 Ensure separate partition exists for /var/log	High	1
1.1.11 Ensure separate partition exists for /var/log/audit	High	1
1.1.12 Ensure separate partition exists for /home	High	1

1.1.16 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 freevxfs filesystems is disabled	High	1
1.1.1.3 Ensure mounting of jffs2 filesystems is disabled	High	1
1.1.1.4 Ensure mounting of hfs filesystems is disabled	High	1
1.1.1.5 Ensure mounting of hfsplus filesystems is disabled	High	1
1.1.1.6 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
1.4.1 Ensure permissions on bootloader config are configured	High	1
1.4.2 Ensure bootloader password is set	High	1
1.5.1 Ensure core dumps are restricted	High	1
1.7.1.4 Ensure permissions on /etc/motd are configured	Informational	1
2.3.4 Ensure telnet client is not installed	High	1
3.1.2 Ensure packet redirect sending is disabled	High	1
3.2.3 Ensure secure ICMP redirects are not accepted	High	1
3.2.4 Ensure suspicious packets are logged	High	1
3.2.8 Ensure TCP SYN Cookies is enabled	High	1
3.3.1 Ensure IPv6 router advertisements are not accepted	Informational	1
3.3.3 Ensure IPv6 is disabled	Informational	1
3.4.3 Ensure /etc/hosts.deny is configured	High	1
3.5.1 Ensure DCCP is disabled	Informational	1
3.5.2 Ensure SCTP is disabled	Informational	1
3.5.3 Ensure RDS is disabled	Informational	1
3.5.4 Ensure TIPC is disabled	Informational	1
3.6.2 Ensure default deny firewall policy	High	1
3.6.3 Ensure loopback traffic is configured	High	1
3.6.5 Ensure firewall rules exist for all open ports	High	1
4.1.2 Ensure auditd service is enabled	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
4.1.1.1 Ensure audit log storage size is configured	Informational	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
4.2.1.4 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
5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured	High	1
5.2.4 Ensure SSH X11 forwarding is disabled	High	1
5.2.5 Ensure SSH MaxAuthTries is set to 4 or less	High	1
5.2.8 Ensure SSH root login is disabled	High	1
5.2.10 Ensure SSH PermitUserEnvironment is disabled	High	1
5.2.11 Ensure only approved MAC algorithms are used	High	1
5.2.12 Ensure SSH Idle Timeout Interval is configured	High	1
5.2.13 Ensure SSH LoginGraceTime is set to one minute or less	High	1
5.2.14 Ensure SSH access is limited	High	1
5.2.15 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	Informational	1
5.3.3 Ensure password reuse is limited	High	1
5.4.2 Ensure system accounts are non-login	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 90 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
6.1.11 Ensure no unowned files or directories exist	High	1
6.1.12 Ensure no ungrouped files or directories exist	High	1
6.2.7 Ensure all users' home directories exist	High	1
6.2.8 Ensure users' home directories permissions are 750 or more restrictive	High	1

3.1.4 Level 2 - Workstation

Rule	Severity	Failed
1.1.2 Ensure separate partition exists for /tmp	High	1
1.1.5 Ensure separate partition exists for /var	High	1
1.1.6 Ensure separate partition exists for /var/tmp	High	1
1.1.10 Ensure separate partition exists for /var/log	High	1
1.1.11 Ensure separate partition exists for /var/log/audit	High	1
1.1.12 Ensure separate partition exists for /home	High	1
1.1.16 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 freevxfs filesystems is disabled	High	1
1.1.1.3 Ensure mounting of jffs2 filesystems is disabled	High	1
1.1.1.4 Ensure mounting of hfs filesystems is disabled	High	1
1.1.1.5 Ensure mounting of hfsplus filesystems is disabled	High	1
1.1.1.6 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
1.4.1 Ensure permissions on bootloader config are configured	High	1
1.4.2 Ensure bootloader password is set	High	1
1.5.1 Ensure core dumps are restricted	High	1
1.7.1.4 Ensure permissions on /etc/motd are configured	Informational	1
2.3.4 Ensure telnet client is not installed	High	1
3.1.2 Ensure packet redirect sending is disabled	High	1
3.2.3 Ensure secure ICMP redirects are not accepted	High	1
3.2.4 Ensure suspicious packets are logged	High	1
3.2.8 Ensure TCP SYN Cookies is enabled	High	1
3.3.1 Ensure IPv6 router advertisements are not accepted	Informational	1
3.3.3 Ensure IPv6 is disabled	Informational	1
3.4.3 Ensure /etc/hosts.deny is configured	High	1
3.5.1 Ensure DCCP is disabled	Informational	1

3.5.2 Ensure SCTP is disabled	Informational	1
3.5.3 Ensure RDS is disabled	Informational	1
3.5.4 Ensure TIPC is disabled	Informational	1
3.6.2 Ensure default deny firewall policy	High	1
3.6.3 Ensure loopback traffic is configured	High	1
3.6.5 Ensure firewall rules exist for all open ports	High	1
4.1.2 Ensure auditd service is enabled	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
4.1.1.1 Ensure audit log storage size is configured	Informational	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
4.2.1.4 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

5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured	High	1
5.2.4 Ensure SSH X11 forwarding is disabled	High	1
5.2.5 Ensure SSH MaxAuthTries is set to 4 or less	High	1
5.2.8 Ensure SSH root login is disabled	High	1
5.2.10 Ensure SSH PermitUserEnvironment is disabled	High	1
5.2.11 Ensure only approved MAC algorithms are used	High	1
5.2.12 Ensure SSH Idle Timeout Interval is configured	High	1
5.2.13 Ensure SSH LoginGraceTime is set to one minute or less	High	1
5.2.14 Ensure SSH access is limited	High	1
5.2.15 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	Informational	1
5.3.3 Ensure password reuse is limited	High	1
5.4.2 Ensure system accounts are non-login	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 90 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
6.1.11 Ensure no unowned files or directories exist	High	1
6.1.12 Ensure no ungrouped files or directories exist	High	1
6.2.7 Ensure all users' home directories exist	High	1
6.2.8 Ensure users' home directories permissions are 750 or more restrictive	High	1

3.2: Findings table - Common Vulnerabilities and Exposures-1.1

Rule	Severity	Failed
CVE-2015-1336	High	1
CVE-2016-2226	High	1
CVE-2016-2779	High	1
CVE-2016-5011	Medium	1
CVE-2016-9840	High	1
CVE-2016-9841	High	1
CVE-2016-9842	High	1
CVE-2016-9843	High	1
CVE-2017-18174	High	1

CVE-2017-9525	High	1
CVE-2018-10880	High	1
CVE-2018-10883	Medium	1
CVE-2018-12896	Medium	1
CVE-2018-13053	Medium	1
CVE-2018-13096	Medium	1
CVE-2018-14609	High	1
CVE-2018-14617	High	1
CVE-2018-16862	Medium	1
CVE-2018-17972	Medium	1
CVE-2018-18021	Medium	1
CVE-2018-18690	Medium	1
CVE-2018-18710	Medium	1
CVE-2018-19407	Medium	1
CVE-2018-19824	Medium	1
CVE-2018-20169	High	1

3.3: Findings table - Network Reachability-1.1

Rule	Severity	Failed
Recognized port with listener reachable from a Virtual Private Gateway	Informational	1
Recognized port with listener reachable from internet	Informational	1
Recognized port with no listener reachable from a Virtual Private Gateway	Informational	1
Recognized port with no listener reachable from internet	Informational	1

3.4: Findings table - Runtime Behavior Analysis-1.0

Rule	Severity	Failed
Insecure server protocols	Informational	1
Unused listening TCP ports	Informational	1

3.5: 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 - Server

1.1.16 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-0f30edc8c6bf5cb5a

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 the file /etc/modprobe.d/CIS.conf and add the following line: install cramfs /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.2 Ensure mounting of freevxfs filesystems is disabled

Severity
High

Description
Description The freevxfs filesystem type is a free version of the Veritas type filesystem. This is the primary filesystem type for HP-UX operating systems. 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 the file /etc/modprobe.d/CIS.conf and add the following line: install freevxfs /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.3 Ensure mounting of jffs2 filesystems is disabled

Severity
High

Description
Description The jffs2 (journaling flash filesystem 2) filesystem type is a log-structured filesystem used in flash memory devices. 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 the file /etc/modprobe.d/CIS.conf and add the following line: install jffs2 /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.4 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 the file /etc/modprobe.d/CIS.conf and add the following line: install hfs /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.5 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 the file /etc/modprobe.d/CIS.conf and add the following line: install hfsplus /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.6 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 the file /etc/modprobe.d/CIS.conf and add the following line: install udf /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

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: # apt-get install aide Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options. Initialize AIDE: # aide --init

Failed Instances
i-0f30edc8c6bf5cb5a

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/bin/aide --check

Failed Instances
i-0f30edc8c6bf5cb5a

1.4.1 Ensure permissions on bootloader config are configured

Severity
High

Description
Description The grub configuration file contains information on boot settings and passwords for unlocking boot options. The grub configuration is usually grub.cfg stored in /boot/grub. Rationale 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.

Recommendation

Run the following commands to set permissions on your grub configuration: # chown root:root /boot/grub/grub.cfg# chmod og-rwx /boot/grub/grub.cfg

Failed Instances
i-0f30edc8c6bf5cb5a

1.4.2 Ensure bootloader password is set

Severity
High

Description
Description Setting the boot loader password will require that anyone rebooting the system must enter a password before being able to set command line boot parameters Rationale Requiring a boot password upon execution of the boot loader will prevent an unauthorized user from entering boot parameters or changing the boot partition. This prevents users from weakening security (e.g. turning off SELinux at boot time).

Recommendation
Create an encrypted password with grub-mkpasswd-pbkdf2: # grub-mkpasswd-pbkdf2Enter password: <password>Reenter password: <password>Your PBKDF2 is <encrypted-password> Add the following into /etc/grub.d/00_header or a custom /etc/grub.d configuration file: cat <<EOFset superusers="<username>"password_pbkdf2 <username><encrypted-password>EOF Run the following command to update the grub2 configuration: # update-grub

Failed Instances
i-0f30edc8c6bf5cb5a

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

Failed Instances
i-0f30edc8c6bf5cb5a

1.7.1.4 Ensure permissions on /etc/motd are configured

Severity
Informational

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. Rationale If the /etc/motd file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Recommendation
Run the following commands to set permissions on /etc/motd: # chown root:root /etc/motd# chmod 644 /etc/motd

Failed Instances
i-0f30edc8c6bf5cb5a

2.3.4 Ensure telnet client is not installed

Severity
High

Description
Description The telnet package contains the telnet client, which allows users to start connections to other systems via the telnet protocol. Rationale 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.

Recommendation
Run the following command to uninstall telnet: # apt-get remove telnet Impact: Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Failed Instances
i-0f30edc8c6bf5cb5a

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 the /etc/sysctl.conf file: net.ipv4.conf.all.send_redirects = 0net.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-0f30edc8c6bf5cb5a

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_redirec ts to 0 protects the system from routing table updates by possibly compromised known gateways.

Recommendation
Set the following parameters in the /etc/sysctl.conf file: net.ipv4.conf.all.secure_redirec ts = 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-0f30edc8c6bf5cb5a

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 the /etc/sysctl.conf file: net.ipv4.conf.all.log_martians = 1net.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.con f.default.log_martians=1# sysctl -w net.ipv4.route.flush=1

Failed Instances
i-0f30edc8c6bf5cb5a

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 parameter in the /etc/sysctl.conf 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-0f30edc8c6bf5cb5a

3.3.1 Ensure IPv6 router advertisements are not accepted

Severity
Informational

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 the /etc/sysctl.conf 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-0f30edc8c6bf5cb5a

3.3.3 Ensure IPv6 is disabled

Severity
Informational

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

Recommendation
Edit /etc/default/grub and add ' ipv6.disable=1' to GRUB_CMDLINE_LINUX: GRUB_CMDLINE_LINUX="ipv6.disable=1" Run the following command to update the grub2 configuration: # update-grub

Failed Instances
i-0f30edc8c6bf5cb5a

3.4.3 Ensure /etc/hosts.deny is configured

Severity
High

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-0f30edc8c6bf5cb5a

3.5.1 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-0f30edc8c6bf5cb5a

3.5.2 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-0f30edc8c6bf5cb5a

3.5.3 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-0f30edc8c6bf5cb5a

3.5.4 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-0f30edc8c6bf5cb5a

3.6.2 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-0f30edc8c6bf5cb5a

3.6.3 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-0f30edc8c6bf5cb5a

3.6.5 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-0f30edc8c6bf5cb5a

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: # chmod -R g-wx,o-rwx /var/log/*

Failed Instances
i-0f30edc8c6bf5cb5a

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 file 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 restart rsyslog: # pkill -HUP rsyslogd

Failed Instances
i-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured

Severity
High

Description
Description The /etc/ssh/sshd_config file contains configuration specifications for sshd. The command below sets the owner and group of the file to root. Rationale The /etc/ssh/sshd_config file needs to be protected from unauthorized changes by non-privileged users.

Recommendation
Run the following commands to set ownership and permissions on /etc/ssh/sshd_config: # chown root:root /etc/ssh/sshd_config# chmod 600 /etc/ssh/sshd_config

Failed Instances
i-0f30edc8c6bf5cb5a

5.2.4 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-0f30edc8c6bf5cb5a

5.2.5 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-0f30edc8c6bf5cb5a

5.2.8 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-0f30edc8c6bf5cb5a

5.2.10 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-0f30edc8c6bf5cb5a

5.2.11 Ensure only approved 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 to set the parameter as follows: MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com

Failed Instances
i-0f30edc8c6bf5cb5a

5.2.12 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 as follows: ClientAliveInterval 300ClientAliveCountMax 0

Failed Instances
i-0f30edc8c6bf5cb5a

5.2.13 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-0f30edc8c6bf5cb5a

5.2.14 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 comma 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 comma 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 comma 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 comma 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-0f30edc8c6bf5cb5a

5.2.15 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-0f30edc8c6bf5cb5a

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 moredcredit=-1 - provide at least one digitucredit=-1 - provide at least one uppercase characterocredit=-1 - provide at least one special characterlcredit=-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

Run the following command to install the pam_pwquality module: apt-get install libpam-pwquality Edit the /etc/pam.d/common-passwd file 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-0f30edc8c6bf5cb5a

5.3.2 Ensure lockout for failed password attempts is configured

Severity
Informational

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/common-auth file and add the auth line below: auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900 Note: If a user has been locked out because they have reached the maximum consecutive failure count defined by deny= in the pam_tally2.so module, the user can be unlocked by issuing the command /sbin/pam_tally2 -u <username> --reset. This command sets the failed count to 0, effectively unlocking the user.

Failed Instances
i-0f30edc8c6bf5cb5a

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/common-password file to include the remember option and conform to site policy as shown: password sufficient pam_unix.so remember=5

Failed Instances
i-0f30edc8c6bf5cb5a

5.4.2 Ensure system accounts are non-login

Severity
High

Description
Description There are a number of accounts provided with Ubuntu that are used to manage applications and are not intended to provide an interactive shell. Rationale 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, Ubuntu 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.

Recommendation
Set the shell for any accounts returned by the audit script to /usr/sbin/nologin: # usermod -s /usr/sbin/nologin <user> The following script will automatically set all user shells required to /usr/sbin/nologin and lock the sync, shutdown, and halt users: #!/bin/bashfor user in `awk -F: '($3 < 1000) {print $1 }' /etc/passwd`; do if [$user != "root"]; then usermod -L $user if [$user != "sync"] && [$user != "shutdown"] && [$user != "halt"]; then usermod -s /usr/sbin/nologin $user fi fidone

Failed Instances
i-0f30edc8c6bf5cb5a

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/bash.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:
umask 027

Failed Instances
i-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

5.4.1.1 Ensure password expiration is 90 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 90 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 90 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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

6.1.11 Ensure no unowned files or directories exist

Severity
High

Description
Description Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system. Rationale A new user

who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Recommendation
Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

Failed Instances
i-0f30edc8c6bf5cb5a

6.1.12 Ensure no ungrouped files or directories exist

Severity
High

Description
Description Sometimes when administrators delete users or groups from the system they neglect to remove all files owned by those users or groups. Rationale A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Recommendation
Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

Failed Instances
i-0f30edc8c6bf5cb5a

6.2.7 Ensure all users' home directories exist

Severity
High

Description
Description Users can be defined in /etc/passwd without a home directory or with a home directory that does not actually exist. Rationale 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.

Recommendation
If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users without an assigned home directory should be removed or assigned a home directory as appropriate.

Failed Instances
i-0f30edc8c6bf5cb5a

6.2.8 Ensure users' home directories permissions are 750 or more restrictive

Severity
High

Description
Description While the system administrator can establish secure permissions for users' home directories, the users can easily override these. Rationale 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.

Recommendation
Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.

Failed Instances
i-0f30edc8c6bf5cb5a

4.1.2 Level 1 - Workstation

1.1.16 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-0f30edc8c6bf5cb5a

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 the file /etc/modprobe.d/CIS.conf and add the following line: install cramfs /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.2 Ensure mounting of freevxfs filesystems is disabled

Severity
High

Description
Description The freevxfs filesystem type is a free version of the Veritas type filesystem. This is the primary filesystem type for HP-UX operating systems. 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 the file /etc/modprobe.d/CIS.conf and add the following line: install freevxfs /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.3 Ensure mounting of jffs2 filesystems is disabled

Severity
High

Description
Description The jffs2 (journaling flash filesystem 2) filesystem type is a log-structured filesystem used in flash memory devices. 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 the file /etc/modprobe.d/CIS.conf and add the following line: install jffs2 /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.4 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 the file /etc/modprobe.d/CIS.conf and add the following line: install hfs /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.5 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 the file /etc/modprobe.d/CIS.conf and add the following line: install hfsplus /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.6 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 the file /etc/modprobe.d/CIS.conf and add the following line: install udf /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

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: # apt-get install aide Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options. Initialize AIDE: # aide --init

Failed Instances
i-0f30edc8c6bf5cb5a

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/bin/aide --check

Failed Instances
i-0f30edc8c6bf5cb5a

1.4.1 Ensure permissions on bootloader config are configured

Severity
High

Description
Description The grub configuration file contains information on boot settings and passwords for unlocking boot options. The grub configuration is usually grub.cfg stored in /boot/grub. Rationale 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.

Recommendation
Run the following commands to set permissions on your grub configuration: # chown root:root /boot/grub/grub.cfg# chmod og-rwx /boot/grub/grub.cfg

Failed Instances
i-0f30edc8c6bf5cb5a

1.4.2 Ensure bootloader password is set

Severity
High

Description
Description Setting the boot loader password will require that anyone rebooting the system must enter a password before being able to set command line boot parameters Rationale Requiring a boot password upon execution of the boot loader will prevent an unauthorized user from entering boot parameters or changing the boot partition. This prevents users from weakening security (e.g. turning off SELinux at boot time).

Recommendation
Create an encrypted password with grub-mkpasswd-pbkdf2: # grub-mkpasswd-pbkdf2Enter password: <password>Reenter password: <password>Your PBKDF2 is <encrypted-password> Add the following into /etc/grub.d/00_header or a custom /etc/grub.d configuration file: cat <<EOFset superusers="<username>"password_pbkdf2 <username><encrypted-password>EOF Run the following command to update the grub2 configuration: # update-grub

Failed Instances
i-0f30edc8c6bf5cb5a

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

Failed Instances
i-0f30edc8c6bf5cb5a

1.7.1.4 Ensure permissions on /etc/motd are configured

Severity
Informational

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. Rationale If the /etc/motd file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Recommendation
Run the following commands to set permissions on /etc/motd: # chown root:root /etc/motd# chmod 644 /etc/motd

Failed Instances
i-0f30edc8c6bf5cb5a

2.3.4 Ensure telnet client is not installed

Severity
High

Description
Description The telnet package contains the telnet client, which allows users to start connections to other systems via the telnet protocol. Rationale 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.

Recommendation
Run the following command to uninstall telnet: # apt-get remove telnet Impact: Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Failed Instances
i-0f30edc8c6bf5cb5a

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 the /etc/sysctl.conf file: net.ipv4.conf.all.send_redirects = 0net.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-0f30edc8c6bf5cb5a

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_redirec ts to 0 protects the system from routing table updates by possibly compromised known gateways.

Recommendation
Set the following parameters in the /etc/sysctl.conf file: net.ipv4.conf.all.secure_redirec ts = 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-0f30edc8c6bf5cb5a

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 the /etc/sysctl.conf file: net.ipv4.conf.all.log_martians = 1net.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.con f.default.log_martians=1# sysctl -w net.ipv4.route.flush=1

Failed Instances

i-0f30edc8c6bf5cb5a

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 parameter in the /etc/sysctl.conf 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-0f30edc8c6bf5cb5a

3.3.1 Ensure IPv6 router advertisements are not accepted

Severity
Informational

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 the /etc/sysctl.conf 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-0f30edc8c6bf5cb5a

3.3.3 Ensure IPv6 is disabled

Severity
Informational

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

Recommendation
Edit /etc/default/grub and add ' ipv6.disable=1' to GRUB_CMDLINE_LINUX: GRUB_CMDLINE_LINUX="ipv6.disable=1" Run the following command to update the grub2 configuration: # update-grub

Failed Instances
i-0f30edc8c6bf5cb5a

3.4.3 Ensure /etc/hosts.deny is configured

Severity
High

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-0f30edc8c6bf5cb5a

3.5.1 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-0f30edc8c6bf5cb5a

3.5.2 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-0f30edc8c6bf5cb5a

3.5.3 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-0f30edc8c6bf5cb5a

3.5.4 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-0f30edc8c6bf5cb5a

3.6.2 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-0f30edc8c6bf5cb5a

3.6.3 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-0f30edc8c6bf5cb5a

3.6.5 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-0f30edc8c6bf5cb5a

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: # chmod -R g-wx,o-rwx /var/log/*

Failed Instances
i-0f30edc8c6bf5cb5a

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 file 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 restart rsyslog: # pkill -HUP rsyslogd

Failed Instances
i-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured

Severity
High

Description
Description The /etc/ssh/sshd_config file contains configuration specifications for sshd. The command below sets the owner and group of the file to root. Rationale The /etc/ssh/sshd_config file needs to be protected from unauthorized changes by non-privileged users.

Recommendation
Run the following commands to set ownership and permissions on /etc/ssh/sshd_config: # chown root:root /etc/ssh/sshd_config# chmod 600 /etc/ssh/sshd_config

Failed Instances
i-0f30edc8c6bf5cb5a

5.2.4 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-0f30edc8c6bf5cb5a

5.2.5 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-0f30edc8c6bf5cb5a

5.2.8 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-0f30edc8c6bf5cb5a

5.2.10 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-0f30edc8c6bf5cb5a

5.2.11 Ensure only approved 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 to set the parameter as follows: MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com

Failed Instances
i-0f30edc8c6bf5cb5a

5.2.12 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 as follows: ClientAliveInterval 300ClientAliveCountMax 0

Failed Instances
i-0f30edc8c6bf5cb5a

5.2.13 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-0f30edc8c6bf5cb5a

5.2.14 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 comma 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 comma 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 comma 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 comma 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-0f30edc8c6bf5cb5a

5.2.15 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-0f30edc8c6bf5cb5a

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 moredcredit=-1 - provide at least one digitucredit=-1 - provide at least one uppercase characterocredit=-1 - provide at least one special characterlcredit=-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
Run the following command to install the pam_pwquality module: apt-get install libpam-pwquality Edit the /etc/pam.d/common-passwd file 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-0f30edc8c6bf5cb5a

5.3.2 Ensure lockout for failed password attempts is configured

Severity
Informational

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/common-auth file and add the auth line below: auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900 Note: If a user has been locked out because they have reached the maximum consecutive failure count defined by deny= in the pam_tally2.so module, the user can be unlocked by issuing the command /sbin/pam_tally2 -u <username> --reset. This command sets the failed count to 0, effectively unlocking the user.

Failed Instances
i-0f30edc8c6bf5cb5a

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/common-password file to include the remember option and conform to site policy as shown: password sufficient pam_unix.so remember=5

Failed Instances
i-0f30edc8c6bf5cb5a

5.4.2 Ensure system accounts are non-login

Severity
High

Description
Description There are a number of accounts provided with Ubuntu that are used to manage applications and are not intended to provide an interactive shell. Rationale 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, Ubuntu 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.

Recommendation
Set the shell for any accounts returned by the audit script to /usr/sbin/nologin: # usermod -s /usr/sbin/nologin <user> The following script will automatically set all user shells required to /usr/sbin/nologin and lock the sync, shutdown, and halt users: #!/bin/

bashfor user in `awk -F: '($3 < 1000) {print $1 }' /etc/passwd`; do if [$user != "root"]; then usermod -L $user if [$user != "sync"] && [$user != "shutdown"] && [$user != "halt"]; then usermod -s /usr/sbin/nologin $user fi fidone

Failed Instances
i-0f30edc8c6bf5cb5a

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/bash.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:
umask 027

Failed Instances
i-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

5.4.1.1 Ensure password expiration is 90 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 90 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 90 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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

6.1.11 Ensure no unowned files or directories exist

Severity
High

Description
Description Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system. Rationale A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Recommendation
Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

Failed Instances
i-0f30edc8c6bf5cb5a

6.1.12 Ensure no ungrouped files or directories exist

Severity
High

Description
Description Sometimes when administrators delete users or groups from the system they neglect to remove all files owned by those users or groups. Rationale A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Recommendation
Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

Failed Instances
i-0f30edc8c6bf5cb5a

6.2.7 Ensure all users' home directories exist

Severity
High

Description

Description Users can be defined in /etc/passwd without a home directory or with a home directory that does not actually exist. Rationale 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.

Recommendation
If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users without an assigned home directory should be removed or assigned a home directory as appropriate.

Failed Instances
i-0f30edc8c6bf5cb5a

6.2.8 Ensure users' home directories permissions are 750 or more restrictive

Severity
High

Description
Description While the system administrator can establish secure permissions for users' home directories, the users can easily override these. Rationale 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.

Recommendation
Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.

Failed Instances
i-0f30edc8c6bf5cb5a

4.1.3 Level 2 - Server

1.1.2 Ensure separate partition exists for /tmp

Severity
High

Description
Description The /tmp directory is a world-writable directory used for temporary storage by all users and some applications. Rationale 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. In addition, 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.

Recommendation
For new installations, during installation create a custom partition setup and specify a separate partition for /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-0f30edc8c6bf5cb5a

1.1.5 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-0f30edc8c6bf5cb5a

1.1.6 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-0f30edc8c6bf5cb5a

1.1.10 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-0f30edc8c6bf5cb5a

1.1.11 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-0f30edc8c6bf5cb5a

1.1.12 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-0f30edc8c6bf5cb5a

1.1.16 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-0f30edc8c6bf5cb5a

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 the file /etc/modprobe.d/CIS.conf and add the following line: install cramfs /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.2 Ensure mounting of freevxfs filesystems is disabled

Severity
High

Description
Description The freevxfs filesystem type is a free version of the Veritas type filesystem. This is the primary filesystem type for HP-UX operating systems. 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 the file /etc/modprobe.d/CIS.conf and add the following line: install freevxfs /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.3 Ensure mounting of jffs2 filesystems is disabled

Severity
High

Description
Description The jffs2 (journaling flash filesystem 2) filesystem type is a log-structured filesystem used in flash memory devices. 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 the file /etc/modprobe.d/CIS.conf and add the following line: install jffs2 /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.4 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 the file /etc/modprobe.d/CIS.conf and add the following line: install hfs /bin/true

Failed Instances

i-0f30edc8c6bf5cb5a

1.1.1.5 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 the file /etc/modprobe.d/CIS.conf and add the following line: install hfsplus /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.6 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 the file /etc/modprobe.d/CIS.conf and add the following line: install udf /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

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: # apt-get install aide Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options. Initialize AIDE: # aide --init

Failed Instances
i-0f30edc8c6bf5cb5a

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/bin/aide --check

Failed Instances
i-0f30edc8c6bf5cb5a

1.4.1 Ensure permissions on bootloader config are configured

Severity
High

Description
Description The grub configuration file contains information on boot settings and passwords for unlocking boot options. The grub configuration is usually grub.cfg stored in /boot/grub. Rationale 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.

Recommendation
Run the following commands to set permissions on your grub configuration: # chown root:root /boot/grub/grub.cfg# chmod og-rwx /boot/grub/grub.cfg

Failed Instances
i-0f30edc8c6bf5cb5a

1.4.2 Ensure bootloader password is set

Severity
High

Description
Description Setting the boot loader password will require that anyone rebooting the system must enter a password before being able to set command line boot parameters Rationale Requiring a boot password upon execution of the boot loader will prevent an unauthorized user from entering boot parameters or changing the boot partition. This prevents users from weakening security (e.g. turning off SELinux at boot time).

Recommendation
Create an encrypted password with grub-mkpasswd-pbkdf2: # grub-mkpasswd-pbkdf2Enter password: <password>Reenter password: <password>Your PBKDF2 is <encrypted-password> Add the following into /etc/grub.d/00_header or a custom /etc/grub.d configuration file: cat <<EOFset superusers="<username>"password_pbkdf2 <username><encrypted-password>EOF Run the following command to update the grub2 configuration: # update-grub

Failed Instances
i-0f30edc8c6bf5cb5a

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

Failed Instances
i-0f30edc8c6bf5cb5a

1.7.1.4 Ensure permissions on /etc/motd are configured

Severity
Informational

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. Rationale If the /etc/motd file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Recommendation
Run the following commands to set permissions on /etc/motd: # chown root:root /etc/motd# chmod 644 /etc/motd

Failed Instances
i-0f30edc8c6bf5cb5a

2.3.4 Ensure telnet client is not installed

Severity
High

Description
Description The telnet package contains the telnet client, which allows users to start connections to other systems via the telnet protocol. Rationale 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.

Recommendation
Run the following command to uninstall telnet: # apt-get remove telnet Impact: Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Failed Instances
i-0f30edc8c6bf5cb5a

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 the /etc/sysctl.conf file: net.ipv4.conf.all.send_redirects = 0net.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-0f30edc8c6bf5cb5a

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 the /etc/sysctl.conf 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-0f30edc8c6bf5cb5a

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 the /etc/sysctl.conf file: net.ipv4.conf.all.log_martians = 1net.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-0f30edc8c6bf5cb5a

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 parameter in the /etc/sysctl.conf 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-0f30edc8c6bf5cb5a

3.3.1 Ensure IPv6 router advertisements are not accepted

Severity
Informational

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 the /etc/sysctl.conf 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-0f30edc8c6bf5cb5a

3.3.3 Ensure IPv6 is disabled

Severity
Informational

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

Recommendation
Edit /etc/default/grub and add ' ipv6.disable=1' to GRUB_CMDLINE_LINUX: GRUB_CMDLINE_LINUX="ipv6.disable=1" Run the following command to update the grub2 configuration: # update-grub

Failed Instances
i-0f30edc8c6bf5cb5a

3.4.3 Ensure /etc/hosts.deny is configured

Severity
High

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-0f30edc8c6bf5cb5a

3.5.1 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-0f30edc8c6bf5cb5a

3.5.2 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-0f30edc8c6bf5cb5a

3.5.3 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-0f30edc8c6bf5cb5a

3.5.4 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-0f30edc8c6bf5cb5a

3.6.2 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-0f30edc8c6bf5cb5a

3.6.3 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-0f30edc8c6bf5cb5a

3.6.5 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-0f30edc8c6bf5cb5a

4.1.2 Ensure auditd service is enabled

Severity
High

Description
Description Turn on the auditd daemon to record system events. Rationale The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Recommendation
Run the following command to enable auditd: # update-rc.d auditd enable

Failed Instances
i-0f30edc8c6bf5cb5a

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: # update-grub

Failed Instances
i-0f30edc8c6bf5cb5a

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), settimeofday (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/audit.rules file: -a always,exit -F arch=b32 -S adjtimex -S settimeofday -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 settimeofday -k time-change-a always,exit -F arch=b32

-S adjtimex -S settimeofday -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-0f30edc8c6bf5cb5a

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/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-0f30edc8c6bf5cb5a

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) and /etc/sysconfig/network (directory containing network interface scripts and configurations) files. 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 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/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/network -p wa -k system-locale-w /etc/networks -p wa -k system-locale
For 64 bit systems add the following lines to the /etc/audit/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/network -p wa -k system-locale-w /etc/networks -p wa -k system-locale

Failed Instances
i-0f30edc8c6bf5cb5a

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

Severity
High

Description
Description Monitor SELinux/AppArmor 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 /etc/apparmor and /etc/apparmor.d directories. 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
On systems using SELinux add the following line to the /etc/audit/audit.rules file: -w /etc/selinux/ -p wa -k MAC-policy On systems using AppArmor add the following line to the /etc/audit/audit.rules file: -w /etc/apparmor/ -p wa -k MAC-policy-w /etc/apparmor.d/ -p wa -k MAC-policy

Failed Instances
i-0f30edc8c6bf5cb5a

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/faillog tracks failed events from login. The file /var/log/lastlog maintain records of the last time a user successfully logged in. The file /var/log/tallylog maintains records of failures via the pam_tally2 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/audit.rules file: -w /var/log/faillog -p wa -k logins-w /var/log/lastlog -p wa -k logins-w /var/log/tallylog -p wa -k logins

Failed Instances
i-0f30edc8c6bf5cb5a

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. The /var/log/wtmp file tracks logins, logouts, shutdown, and reboot events. All audit records will be tagged with the identifier "session." 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/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-0f30edc8c6bf5cb5a

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/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/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-0f30edc8c6bf5cb5a

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/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/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=-EACCES -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-0f30edc8c6bf5cb5a

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/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/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-0f30edc8c6bf5cb5a

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/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/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-0f30edc8c6bf5cb5a

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/audit.rules file: -w /etc/sudoers -p wa -k scope-w /etc/sudoers.d/ -p wa -k scope

Failed Instances
i-0f30edc8c6bf5cb5a

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/audit.rules file: -w /var/log/sudo.log -p wa -k actions

Failed Instances
i-0f30edc8c6bf5cb5a

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/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 arch=b32 -S init_module -S delete_module -k modules For 64 bit systems add the following lines to the /etc/audit/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 arch=b64 -S init_module -S delete_module -k modules

Failed Instances
i-0f30edc8c6bf5cb5a

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/audit.rules file. -e 2

Failed Instances
i-0f30edc8c6bf5cb5a

4.1.1.1 Ensure audit log storage size is configured

Severity
Informational

Description
Description 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. Rationale 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.

Recommendation
Set the following parameter in /etc/audit/auditd.conf in accordance with site policy: max_log_file = <MB>

Failed Instances
i-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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: # chmod -R g-wx,o-rwx /var/log/*

Failed Instances
i-0f30edc8c6bf5cb5a

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 file 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 restart rsyslog: # pkill -HUP rsyslogd

Failed Instances
i-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured

Severity
High

Description
Description The /etc/ssh/sshd_config file contains configuration specifications for sshd. The command below sets the owner and group of the file to root. Rationale The /etc/ssh/sshd_config file needs to be protected from unauthorized changes by non-privileged users.

Recommendation
Run the following commands to set ownership and permissions on /etc/ssh/sshd_config: # chown root:root /etc/ssh/sshd_config# chmod 600 /etc/ssh/sshd_config

Failed Instances
i-0f30edc8c6bf5cb5a

5.2.4 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-0f30edc8c6bf5cb5a

5.2.5 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-0f30edc8c6bf5cb5a

5.2.8 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-0f30edc8c6bf5cb5a

5.2.10 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-0f30edc8c6bf5cb5a

5.2.11 Ensure only approved 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 to set the parameter as follows: MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com

Failed Instances
i-0f30edc8c6bf5cb5a

5.2.12 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 as follows: ClientAliveInterval 300ClientAliveCountMax 0

Failed Instances
i-0f30edc8c6bf5cb5a

5.2.13 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-0f30edc8c6bf5cb5a

5.2.14 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 comma 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 comma 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 comma 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 comma 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-0f30edc8c6bf5cb5a

5.2.15 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-0f30edc8c6bf5cb5a

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 moredcredit=-1 - provide at least one digitucredit=-1 - provide at least one uppercase characterocredit=-1 - provide at least one special characterlcredit=-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

Run the following command to install the pam_pwquality module: apt-get install libpam-pwquality Edit the /etc/pam.d/common-passwd file 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-0f30edc8c6bf5cb5a

5.3.2 Ensure lockout for failed password attempts is configured

Severity
Informational

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/common-auth file and add the auth line below: auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900 Note: If a user has been locked out because they have reached the maximum consecutive failure count defined by deny= in the pam_tally2.so module, the user can be unlocked by issuing the command /sbin/pam_tally2 -u <username> --reset. This command sets the failed count to 0, effectively unlocking the user.

Failed Instances
i-0f30edc8c6bf5cb5a

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/common-password file to include the remember option and conform to site policy as shown: password sufficient pam_unix.so remember=5

Failed Instances
i-0f30edc8c6bf5cb5a

5.4.2 Ensure system accounts are non-login

Severity
High

Description
Description There are a number of accounts provided with Ubuntu that are used to manage applications and are not intended to provide an interactive shell. Rationale 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, Ubuntu 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.

Recommendation
Set the shell for any accounts returned by the audit script to /usr/sbin/nologin: # usermod -s /usr/sbin/nologin <user> The following script will automatically set all user shells required to /usr/sbin/nologin and lock the sync, shutdown, and halt users: #!/bin/bashfor user in `awk -F: '($3 < 1000) {print $1 }' /etc/passwd`; do if [$user != "root"]; then usermod -L $user if [$user != "sync"] && [$user != "shutdown"] && [$user != "halt"]; then usermod -s /usr/sbin/nologin $user fi fidone

Failed Instances
i-0f30edc8c6bf5cb5a

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/bash.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:
umask 027

Failed Instances
i-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

5.4.1.1 Ensure password expiration is 90 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 90 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 90 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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

6.1.11 Ensure no unowned files or directories exist

Severity
High

Description
Description Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system. Rationale A new user

who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Recommendation
Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

Failed Instances
i-0f30edc8c6bf5cb5a

6.1.12 Ensure no ungrouped files or directories exist

Severity
High

Description
Description Sometimes when administrators delete users or groups from the system they neglect to remove all files owned by those users or groups. Rationale A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Recommendation
Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

Failed Instances
i-0f30edc8c6bf5cb5a

6.2.7 Ensure all users' home directories exist

Severity
High

Description
Description Users can be defined in /etc/passwd without a home directory or with a home directory that does not actually exist. Rationale 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.

Recommendation
If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users without an assigned home directory should be removed or assigned a home directory as appropriate.

Failed Instances
i-0f30edc8c6bf5cb5a

6.2.8 Ensure users' home directories permissions are 750 or more restrictive

Severity
High

Description
Description While the system administrator can establish secure permissions for users' home directories, the users can easily override these. Rationale 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.

Recommendation
Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.

Failed Instances
i-0f30edc8c6bf5cb5a

4.1.4 Level 2 - Workstation

1.1.2 Ensure separate partition exists for /tmp

Severity
High

Description
Description The /tmp directory is a world-writable directory used for temporary storage by all users and some applications. Rationale 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. In addition, 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.

Recommendation
For new installations, during installation create a custom partition setup and specify a separate partition for /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-0f30edc8c6bf5cb5a

1.1.5 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-0f30edc8c6bf5cb5a

1.1.6 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-0f30edc8c6bf5cb5a

1.1.10 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-0f30edc8c6bf5cb5a

1.1.11 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-0f30edc8c6bf5cb5a

1.1.12 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-0f30edc8c6bf5cb5a

1.1.16 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-0f30edc8c6bf5cb5a

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 the file /etc/modprobe.d/CIS.conf and add the following line: install cramfs /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.2 Ensure mounting of freevxfs filesystems is disabled

Severity
High

Description
Description The freevxfs filesystem type is a free version of the Veritas type filesystem. This is the primary filesystem type for HP-UX operating systems. 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 the file /etc/modprobe.d/CIS.conf and add the following line: install freevxfs /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.3 Ensure mounting of jffs2 filesystems is disabled

Severity
High

Description
Description The jffs2 (journaling flash filesystem 2) filesystem type is a log-structured filesystem used in flash memory devices. 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 the file /etc/modprobe.d/CIS.conf and add the following line: install jffs2 /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.4 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 the file /etc/modprobe.d/CIS.conf and add the following line: install hfs /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.5 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 the file /etc/modprobe.d/CIS.conf and add the following line: install hfsplus /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

1.1.1.6 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 the file /etc/modprobe.d/CIS.conf and add the following line: install udf /bin/true

Failed Instances
i-0f30edc8c6bf5cb5a

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: # apt-get install aide Configure AIDE as appropriate for your environment. Consult the AIDE documentation for options. Initialize AIDE: # aide --init

Failed Instances
i-0f30edc8c6bf5cb5a

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/bin/aide --check

Failed Instances
i-0f30edc8c6bf5cb5a

1.4.1 Ensure permissions on bootloader config are configured

Severity
High

Description

Description The grub configuration file contains information on boot settings and passwords for unlocking boot options. The grub configuration is usually grub.cfg stored in /boot/grub. Rationale 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.

Recommendation
Run the following commands to set permissions on your grub configuration: # chown root:root /boot/grub/grub.cfg# chmod og-rwx /boot/grub/grub.cfg

Failed Instances
i-0f30edc8c6bf5cb5a

1.4.2 Ensure bootloader password is set

Severity
High

Description
Description Setting the boot loader password will require that anyone rebooting the system must enter a password before being able to set command line boot parameters Rationale Requiring a boot password upon execution of the boot loader will prevent an unauthorized user from entering boot parameters or changing the boot partition. This prevents users from weakening security (e.g. turning off SELinux at boot time).

Recommendation
Create an encrypted password with grub-mkpasswd-pbkdf2: # grub-mkpasswd-pbkdf2Enter password: <password>Reenter password: <password>Your PBKDF2 is <encrypted-password> Add the following into /etc/grub.d/00_header or a custom /etc/grub.d configuration file: cat <<EOFset superusers="<username>"password_pbkdf2 <username><encrypted-password>EOF Run the following command to update the grub2 configuration: # update-grub

Failed Instances
i-0f30edc8c6bf5cb5a

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

Failed Instances
i-0f30edc8c6bf5cb5a

1.7.1.4 Ensure permissions on /etc/motd are configured

Severity
Informational

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. Rationale If the /etc/motd file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

Recommendation
Run the following commands to set permissions on /etc/motd: # chown root:root /etc/motd# chmod 644 /etc/motd

Failed Instances
i-0f30edc8c6bf5cb5a

2.3.4 Ensure telnet client is not installed

Severity
High

Description
Description The telnet package contains the telnet client, which allows users to start connections to other systems via the telnet protocol. Rationale 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.

Recommendation
Run the following command to uninstall telnet: # apt-get remove telnet Impact: Many insecure service clients are used as troubleshooting tools and in testing environments. Uninstalling them can inhibit capability to test and troubleshoot. If they are required it is advisable to remove the clients after use to prevent accidental or intentional misuse.

Failed Instances
i-0f30edc8c6bf5cb5a

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 the /etc/sysctl.conf file: net.ipv4.conf.all.send_redirects = 0net.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-0f30edc8c6bf5cb5a

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_redirec ts to 0 protects the system from routing table updates by possibly compromised known gateways.

Recommendation
Set the following parameters in the /etc/sysctl.conf file: net.ipv4.conf.all.secure_redirec ts = 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-0f30edc8c6bf5cb5a

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 the /etc/sysctl.conf file: net.ipv4.conf.all.log_martians = 1net.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.con f.default.log_martians=1# sysctl -w net.ipv4.route.flush=1

Failed Instances

i-0f30edc8c6bf5cb5a

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 parameter in the /etc/sysctl.conf 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-0f30edc8c6bf5cb5a

3.3.1 Ensure IPv6 router advertisements are not accepted

Severity
Informational

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 the /etc/sysctl.conf 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-0f30edc8c6bf5cb5a

3.3.3 Ensure IPv6 is disabled

Severity
Informational

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

Recommendation
Edit /etc/default/grub and add ' ipv6.disable=1' to GRUB_CMDLINE_LINUX: GRUB_CMDLINE_LINUX="ipv6.disable=1" Run the following command to update the grub2 configuration: # update-grub

Failed Instances
i-0f30edc8c6bf5cb5a

3.4.3 Ensure /etc/hosts.deny is configured

Severity
High

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-0f30edc8c6bf5cb5a

3.5.1 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-0f30edc8c6bf5cb5a

3.5.2 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-0f30edc8c6bf5cb5a

3.5.3 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-0f30edc8c6bf5cb5a

3.5.4 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-0f30edc8c6bf5cb5a

3.6.2 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-0f30edc8c6bf5cb5a

3.6.3 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-0f30edc8c6bf5cb5a

3.6.5 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-0f30edc8c6bf5cb5a

4.1.2 Ensure auditd service is enabled

Severity
High

Description
Description Turn on the auditd daemon to record system events. Rationale The capturing of system events provides system administrators with information to allow them to determine if unauthorized access to their system is occurring.

Recommendation
Run the following command to enable auditd: # update-rc.d auditd enable

Failed Instances
i-0f30edc8c6bf5cb5a

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: # update-grub

Failed Instances
i-0f30edc8c6bf5cb5a

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), settimeofday (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/audit.rules file: -a always,exit -F arch=b32 -S adjtimex -S settimeofday -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 settimeofday -k time-change-a always,exit -F arch=b32

-S adjtimex -S settimeofday -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-0f30edc8c6bf5cb5a

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/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-0f30edc8c6bf5cb5a

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) and /etc/sysconfig/network (directory containing network interface scripts and configurations) files. 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 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/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/network -p wa -k system-locale-w /etc/networks -p wa -k system-locale
For 64 bit systems add the following lines to the /etc/audit/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/network -p wa -k system-locale-w /etc/networks -p wa -k system-locale

Failed Instances
i-0f30edc8c6bf5cb5a

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

Severity
High

Description
Description Monitor SELinux/AppArmor 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 /etc/apparmor and /etc/apparmor.d directories. 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
On systems using SELinux add the following line to the /etc/audit/audit.rules file: -w /etc/selinux/ -p wa -k MAC-policy On systems using AppArmor add the following line to the /etc/audit/audit.rules file: -w /etc/apparmor/ -p wa -k MAC-policy-w /etc/apparmor.d/ -p wa -k MAC-policy

Failed Instances
i-0f30edc8c6bf5cb5a

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/faillog tracks failed events from login. The file /var/log/lastlog maintain records of the last time a user successfully logged in. The file /var/log/tallylog maintains records of failures via the pam_tally2 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/audit.rules file: -w /var/log/faillog -p wa -k logins-w /var/log/lastlog -p wa -k logins-w /var/log/tallylog -p wa -k logins

Failed Instances
i-0f30edc8c6bf5cb5a

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. The /var/log/wtmp file tracks logins, logouts, shutdown, and reboot events. All audit records will be tagged with the identifier "session." 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/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-0f30edc8c6bf5cb5a

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/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/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-0f30edc8c6bf5cb5a

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/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/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=-EACCES -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-0f30edc8c6bf5cb5a

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/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/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-0f30edc8c6bf5cb5a

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/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/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-0f30edc8c6bf5cb5a

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/audit.rules file: -w /etc/sudoers -p wa -k scope-w /etc/sudoers.d/ -p wa -k scope

Failed Instances
i-0f30edc8c6bf5cb5a

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/audit.rules file: -w /var/log/sudo.log -p wa -k actions

Failed Instances
i-0f30edc8c6bf5cb5a

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/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 arch=b32 -S init_module -S delete_module -k modules For 64 bit systems add the following lines to the /etc/audit/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 arch=b64 -S init_module -S delete_module -k modules

Failed Instances
i-0f30edc8c6bf5cb5a

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/audit.rules file. -e 2

Failed Instances
i-0f30edc8c6bf5cb5a

4.1.1.1 Ensure audit log storage size is configured

Severity
Informational

Description
Description 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. Rationale 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.

Recommendation
Set the following parameter in /etc/audit/auditd.conf in accordance with site policy: max_log_file = <MB>

Failed Instances
i-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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: # chmod -R g-wx,o-rwx /var/log/*

Failed Instances
i-0f30edc8c6bf5cb5a

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 file 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 restart rsyslog: # pkill -HUP rsyslogd

Failed Instances
i-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

5.2.1 Ensure permissions on /etc/ssh/sshd_config are configured

Severity
High

Description
Description The /etc/ssh/sshd_config file contains configuration specifications for sshd. The command below sets the owner and group of the file to root. Rationale The /etc/ssh/sshd_config file needs to be protected from unauthorized changes by non-privileged users.

Recommendation
Run the following commands to set ownership and permissions on /etc/ssh/sshd_config: # chown root:root /etc/ssh/sshd_config# chmod 600 /etc/ssh/sshd_config

Failed Instances
i-0f30edc8c6bf5cb5a

5.2.4 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-0f30edc8c6bf5cb5a

5.2.5 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-0f30edc8c6bf5cb5a

5.2.8 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-0f30edc8c6bf5cb5a

5.2.10 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-0f30edc8c6bf5cb5a

5.2.11 Ensure only approved 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 to set the parameter as follows: MACs hmac-sha2-512-etm@openssh.com,hmac-sha2-256-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-512,hmac-sha2-256,umac-128@openssh.com

Failed Instances
i-0f30edc8c6bf5cb5a

5.2.12 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 as follows: ClientAliveInterval 300ClientAliveCountMax 0

Failed Instances
i-0f30edc8c6bf5cb5a

5.2.13 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-0f30edc8c6bf5cb5a

5.2.14 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 comma 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 comma 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 comma 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 comma 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-0f30edc8c6bf5cb5a

5.2.15 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-0f30edc8c6bf5cb5a

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 moredcredit=-1 - provide at least one digitucredit=-1 - provide at least one uppercase characterocredit=-1 - provide at least one special characterlcredit=-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

Run the following command to install the pam_pwquality module: apt-get install libpam-pwquality Edit the /etc/pam.d/common-passwd file 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-0f30edc8c6bf5cb5a

5.3.2 Ensure lockout for failed password attempts is configured

Severity
Informational

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/common-auth file and add the auth line below: auth required pam_tally2.so onerr=fail audit silent deny=5 unlock_time=900 Note: If a user has been locked out because they have reached the maximum consecutive failure count defined by deny= in the pam_tally2.so module, the user can be unlocked by issuing the command /sbin/pam_tally2 -u <username> --reset. This command sets the failed count to 0, effectively unlocking the user.

Failed Instances
i-0f30edc8c6bf5cb5a

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/common-password file to include the remember option and conform to site policy as shown: password sufficient pam_unix.so remember=5

Failed Instances
i-0f30edc8c6bf5cb5a

5.4.2 Ensure system accounts are non-login

Severity
High

Description
Description There are a number of accounts provided with Ubuntu that are used to manage applications and are not intended to provide an interactive shell. Rationale 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, Ubuntu 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.

Recommendation
Set the shell for any accounts returned by the audit script to /usr/sbin/nologin: # usermod -s /usr/sbin/nologin <user> The following script will automatically set all user shells required to /usr/sbin/nologin and lock the sync, shutdown, and halt users: #!/bin/bashfor user in `awk -F: '($3 < 1000) {print $1 }' /etc/passwd`; do if [$user != "root"]; then usermod -L $user if [$user != "sync"] && [$user != "shutdown"] && [$user != "halt"]; then usermod -s /usr/sbin/nologin $user fi fidone

Failed Instances
i-0f30edc8c6bf5cb5a

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/bash.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:
umask 027

Failed Instances
i-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

5.4.1.1 Ensure password expiration is 90 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 90 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 90 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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

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-0f30edc8c6bf5cb5a

6.1.11 Ensure no unowned files or directories exist

Severity
High

Description
Description Sometimes when administrators delete users from the password file they neglect to remove all files owned by those users from the system. Rationale A new user

who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Recommendation
Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

Failed Instances
i-0f30edc8c6bf5cb5a

6.1.12 Ensure no ungrouped files or directories exist

Severity
High

Description
Description Sometimes when administrators delete users or groups from the system they neglect to remove all files owned by those users or groups. Rationale A new user who is assigned the deleted user's user ID or group ID may then end up "owning" these files, and thus have more access on the system than was intended.

Recommendation
Locate files that are owned by users or groups not listed in the system configuration files, and reset the ownership of these files to some active user on the system as appropriate.

Failed Instances
i-0f30edc8c6bf5cb5a

6.2.7 Ensure all users' home directories exist

Severity
High

Description
Description Users can be defined in /etc/passwd without a home directory or with a home directory that does not actually exist. Rationale 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.

Recommendation
If any users' home directories do not exist, create them and make sure the respective user owns the directory. Users without an assigned home directory should be removed or assigned a home directory as appropriate.

Failed Instances
i-0f30edc8c6bf5cb5a

6.2.8 Ensure users' home directories permissions are 750 or more restrictive

Severity
High

Description
Description While the system administrator can establish secure permissions for users' home directories, the users can easily override these. Rationale 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.

Recommendation
Making global modifications to user home directories without alerting the user community can result in unexpected outages and unhappy users. Therefore, it is recommended that a monitoring policy be established to report user file permissions and determine the action to be taken in accordance with site policy.

Failed Instances
i-0f30edc8c6bf5cb5a

4.2: Findings details - Common Vulnerabilities and Exposures-1.1

CVE-2015-1336

Severity
High

Description

The daily mandb cleanup job in Man-db before 2.7.6.1-1 as packaged in Ubuntu and Debian allows local users with access to the man account to gain privileges via vectors involving insecure chown use.

Recommendation
Use your Operating System's update feature to update package man-db-0:2.7.5-1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1336

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2016-2226

Severity
High

Description
Integer overflow in the string_appends function in cplus-dem.c in libiberty allows remote attackers to execute arbitrary code via a crafted executable, which triggers a buffer overflow.

Recommendation
Use your Operating System's update feature to update package binutils-0:2.26.1-1ubuntu1~16.04.6. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2226

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2016-2779

Severity
High

Description
runuser in util-linux allows local users to escape to the parent session via a crafted TIOCSTI ioctl call, which pushes characters to the terminal's input buffer.

Recommendation

Use your Operating System's update feature to update package util-linux-0:2.27.1-6ubuntu3.6. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-2779

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2016-5011

Severity
Medium

Description
The parse_dos_extended function in partitions/dos.c in the libblkid library in util-linux allows physically proximate attackers to cause a denial of service (memory consumption) via a crafted MSDOS partition table with an extended partition boot record at zero offset.

Recommendation
Use your Operating System's update feature to update package util-linux-0:2.27.1-6ubuntu3.6. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5011

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2016-9840

Severity
High

Description
inftrees.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic.

Recommendation
Use your Operating System's update feature to update package zlib1g-1:1.2.8.dfsg-2ubuntu4.1, zlib1g-dev-1:1.2.8.dfsg-2ubuntu4.1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9840

Failed Instances

i-0f30edc8c6bf5cb5a

CVE-2016-9841

Severity
High

Description
inffast.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic.

Recommendation
Use your Operating System's update feature to update package zlib1g-1:1.2.8.dfsg-2ubuntu4.1, zlib1g-dev-1:1.2.8.dfsg-2ubuntu4.1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9841

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2016-9842

Severity
High

Description
The inflateMark function in inflate.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving left shifts of negative integers.

Recommendation
Use your Operating System's update feature to update package zlib1g-1:1.2.8.dfsg-2ubuntu4.1, zlib1g-dev-1:1.2.8.dfsg-2ubuntu4.1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9842

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2016-9843

Severity

High

Description
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.

Recommendation
Use your Operating System's update feature to update package zlib1g-1:1.2.8.dfsg-2ubuntu4.1, zlib1g-dev-1:1.2.8.dfsg-2ubuntu4.1. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9843

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2017-18174

Severity
High

Description
In the Linux kernel before 4.7, the amd_gpio_remove function in drivers/pinctrl/pinctrl-amd.c calls the pinctrl_unregister function, leading to a double free.

Recommendation
Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80, linux-image-4.4.0-1072-aws-0:4.4.0-1072.82. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-18174

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2017-9525

Severity
High

Description
In the cron package through 3.0pl1-128 on Debian, and through 3.0pl1-128ubuntu2 on Ubuntu, the postinst maintainer script allows for group-crontab-to-root privilege escalation via symlink attacks against unsafe usage of the chown and chmod programs.

Recommendation
Use your Operating System's update feature to update package cron-0:3.0pl1-128ubuntu2. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-9525

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2018-10880

Severity
High

Description
Linux kernel is vulnerable to a stack-out-of-bounds write in the ext4 filesystem code when mounting and writing to a crafted ext4 image in ext4_update_inline_data(). An attacker could use this to cause a system crash and a denial of service.

Recommendation
Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10880

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2018-10883

Severity
Medium

Description
A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bounds write in jbd2_journal_dirty_metadata(), a denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.

Recommendation
Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80, linux-image-4.4.0-1072-aws-0:4.4.0-1072.82, linux-image-4.4.

0-1074-aws-0:4.4.0-1074.84. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-10883

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2018-12896

Severity
Medium

Description
An issue was discovered in the Linux kernel through 4.17.3. An Integer Overflow in kernel/time/posix-timers.c in the POSIX timer code is caused by the way the overrun accounting works. Depending on interval and expiry time values, the overrun can be larger than INT_MAX, but the accounting is int based. This basically makes the accounting values, which are visible to user space via timer_getoverrun(2) and siginfo::si_overrun, random. For example, a local user can cause a denial of service (signed integer overflow) via crafted mmap, futex, timer_create, and timer_settime system calls.

Recommendation
Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80, linux-image-4.4.0-1072-aws-0:4.4.0-1072.82. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-12896

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2018-13053

Severity
Medium

Description
The alarm_timer_nsleep function in kernel/time/alarmtimer.c in the Linux kernel through 4.17.3 has an integer overflow via a large relative timeout because ktime_add_safe is not used.

Recommendation

Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13053

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2018-13096

Severity
Medium

Description
An issue was discovered in fs/f2fs/super.c in the Linux kernel through 4.17.3. A denial of service (out-of-bounds memory access and BUG) can occur upon encountering an abnormal bitmap size when mounting a crafted f2fs image.

Recommendation
Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13096

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2018-14609

Severity
High

Description
An issue was discovered in the Linux kernel through 4.17.10. There is an invalid pointer dereference in __del_reloc_root() in fs/btrfs/relocation.c when mounting a crafted btrfs image, related to removing reloc rb_trees when reloc control has not been initialized.

Recommendation
Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14609

Failed Instances

i-0f30edc8c6bf5cb5a

CVE-2018-14617

Severity
High

Description
An issue was discovered in the Linux kernel through 4.17.10. There is a NULL pointer dereference and panic in hfsplus_lookup() in fs/hfsplus/dir.c when opening a file (that is purportedly a hard link) in an hfs+ filesystem that has malformed catalog data, and is mounted read-only without a metadata directory.

Recommendation
Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-14617

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2018-16862

Severity
Medium

Description
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.

Recommendation
Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80, linux-image-4.4.0-1072-aws-0:4.4.0-1072.82, linux-image-4.4.0-1074-aws-0:4.4.0-1074.84. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-16862

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2018-17972

Severity
Medium

Description
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.

Recommendation
Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17972

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2018-18021

Severity
Medium

Description
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.

Recommendation
Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18021

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2018-18690

Severity
Medium

Description
In the Linux kernel before 4.17, a local attacker able to set attributes on an xfs filesystem could make this filesystem non-operational until the next mount by triggering an unchecked error condition during an xfs attribute change, because xfs_attr_shortform_addname in fs/xfs/libxfs/xfs_attr.c mishandles ATTR_REPLACE operations with conversion of an attr from short to long form.

Recommendation
Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80, linux-image-4.4.0-1072-aws-0:4.4.0-1072.82. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18690

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2018-18710

Severity
Medium

Description
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.

Recommendation
Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80, linux-image-4.4.0-1072-aws-0:4.4.0-1072.82. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-18710

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2018-19407

Severity
Medium

Description
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.

Recommendation
Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80, linux-image-4.4.0-1072-aws-0:4.4.0-1072.82, linux-image-4.4.0-1074-aws-0:4.4.0-1074.84. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19407

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2018-19824

Severity
Medium

Description
In the Linux kernel through 4.19.6, a local user could exploit a use-after-free in the ALSA driver by supplying a malicious USB Sound device (with zero interfaces) that is mishandled in usb_audio_probe in sound/usb/card.c.

Recommendation
Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80, linux-image-4.4.0-1072-aws-0:4.4.0-1072.82, linux-image-4.4.0-1074-aws-0:4.4.0-1074.84. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-19824

Failed Instances
i-0f30edc8c6bf5cb5a

CVE-2018-20169

Severity
High

Description
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.

Recommendation
Use your Operating System's update feature to update package linux-image-4.4.0-1070-aws-0:4.4.0-1070.80, linux-image-4.4.0-1072-aws-0:4.4.0-1072.82, linux-image-4.4.0-1074-aws-0:4.4.0-1074.84. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-20169

Failed Instances
i-0f30edc8c6bf5cb5a

4.3: Findings details - Network Reachability-1.1

Recognized port with listener reachable from a Virtual Private Gateway

Severity
Informational

Description
A recognized port is reachable from a Virtual Private Gateway with a service listening

Recommendation
You can edit the Security Group sg-0a6a8e0d9cc2410a1 to remove access from a Virtual Private Gateway on port 22

Failed Instances
i-0f30edc8c6bf5cb5a

Recognized port with listener reachable from internet

Severity
Informational

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

Recommendation

You can edit the Security Group sg-0a6a8e0d9cc2410a1 to remove access from the internet on port 22

Failed Instances
i-0f30edc8c6bf5cb5a

Recognized port with no listener reachable from a Virtual Private Gateway

Severity
Informational

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

Recommendation
You can edit the Security Group sg-0a6a8e0d9cc2410a1 to remove access from a Virtual Private Gateway on port 443, 80

Failed Instances
i-0f30edc8c6bf5cb5a

Recognized port with no listener reachable from internet

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-0a6a8e0d9cc2410a1 to remove access from the internet on port 443, 80

Failed Instances
i-0f30edc8c6bf5cb5a

4.4: Findings details - Runtime Behavior Analysis-1.0

Insecure server protocols

Severity
Informational

Description
This rule helps determine whether your EC2 instances are hosting insecure services such as FTP, Telnet, HTTP, IMAP, POP version 3, SMTP, SNMP versions 1 and 2, rsh, and rlogin.

Recommendation
We recommend you disable insecure protocols in your assessment target and replace them with secure alternatives as listed below: - Disable telnet, rsh, and rlogin and replace them with SSH. Where this is not possible, you should ensure that the insecure service is protected by appropriate network access controls such as VPC network ACLs and EC2 security groups. - Replace FTP with SCP or SFTP where possible. Where this is not possible, you should ensure that the FTP server is protected by appropriate network access controls such as VPC network ACLs and EC2 security groups. - Replace HTTP with HTTPS where possible. For more information specific to the web server in question see http://nginx.org/en/docs/http/configuring_https_servers.html and https://httpd.apache.org/docs/2.4/ssl/ssl_howto.html. - Disable IMAP, POP3, SMTP services if not required. If required, it's recommended these email protocols should be used with encrypted protocols such as TLS. - Disable SNMP service if not required. If required, replace SNMP v1, v2 with more secure SNMP v3 which uses encrypted communication.

Failed Instances
i-0f30edc8c6bf5cb5a

Unused listening TCP ports

Severity
Informational

Description
This rule detects listening TCP ports that may not be required by the assessment target.

Recommendation
To reduce the attack surface area of your deployments, we recommend that you disable network services that you do not use. Where network services are required, we

recommend that you employ network control mechanisms such as VPC ACLs, EC2 security groups, and firewalls to limit exposure of that service.

Failed Instances
i-0f30edc8c6bf5cb5a

4.5: 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-0f30edc8c6bf5cb5a

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 - Server

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

1.1.7 Ensure nodev option set on /var/tmp partition	Description The nodev mount option specifies that the filesystem cannot contain special devices. Rationale 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.
1.1.8 Ensure nosuid option set on /var/tmp partition	Description The nosuid mount option specifies that the filesystem cannot contain setuid files. Rationale 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.
1.1.9 Ensure noexec option set on /var/tmp partition	Description The noexec mount option specifies that the filesystem cannot contain executable binaries. Rationale 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.

1.1.13 Ensure nodev option set on /home partition	Description The nodev mount option specifies that the filesystem cannot contain special devices. Rationale 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.
1.1.14 Ensure nodev option set on /dev/shm partitiov	Description The nodev mount option specifies that the filesystem cannot contain special devices. Rationale Since the /run/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.
1.1.15 Ensure nosuid option set on /dev/shm partitionrun	Description The nosuid mount option specifies that the filesystem cannot contain setuid files. Rationale Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.

1.1.20 Ensure sticky bit is set on all world-writable directories	Description Setting the sticky bit on world writable directories prevents users from deleting or renaming files in that directory that are not owned by them. Rationale This feature prevents the ability to delete or rename files in world writable directories (such as /tmp) that are owned by another user.
1.1.21 Disable Automounting	Description autofs allows automatic mounting of devices, typically including CD/DVDs and USB drives. Rationale With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.
1.5.2 Ensure XD/NX support is enabled	Description Recent processors in the x86 family support the ability to prevent code execution on a per memory page basis. Generically and on AMD processors, this ability is called No Execute (NX), while on Intel processors it is called Execute Disable (XD). This ability can help prevent exploitation of buffer overflow vulnerabilities and should be activated whenever possible. Extra steps must be taken to ensure that this protection is enabled, particularly on 32-bit x86 systems. Other processors, such as Itanium and POWER, have included such

	support since inception and the standard kernel for those platforms supports the feature. Rationale Enabling any feature that can protect against buffer overflow attacks enhances the security of the system.
1.5.3 Ensure address space layout randomization (ASLR) is enabled	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.
1.5.4 Ensure prelink is disabled	Description 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. Rationale 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.
1.7.2 Ensure GDM login banner is configured	Description GDM is the GNOME Display Manager which handles graphical login for GNOME based systems. 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.
1.7.1.1 Ensure message of the day is configured properly	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.
1.7.1.2 Ensure local login warning banner is configured properly	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.
1.7.1.3 Ensure remote login warning banner is configured properly	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.

1.7.1.5 Ensure permissions on /etc/issue are configured	Description The contents of the /etc/issue file are displayed to users prior to login for local terminals. Rationale If the /etc/issue file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.
1.7.1.6 Ensure permissions on /etc/issue.net are configured	Description The contents of the /etc/issue.net file are displayed to users prior to login for remote connections from configured services. Rationale If the /etc/issue.net file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.
2.1.10 Ensure xinetd is not enabled	Description The eXtended InterNET Daemon (xinetd) is an open source super daemon that replaced the original inetd daemon. The xinetd daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests. Rationale

	If there are no xinetd services required, it is recommended that the daemon be disabled.
2.2.2 Ensure X Window System is not installed	Description 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. Rationale Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface.
2.2.3 Ensure Avahi Server is not enabled	Description Avahi is a free zeroconf implementation, including a system for multicast DNS/DNS-SD service discovery. Avahi allows programs to publish and discover services and hosts running on a local network with no specific configuration. For example, a user can plug a computer into a network and Avahi automatically finds printers to print to, files to look at and people to talk to, as well as network services running on the machine. Rationale Automatic discovery of network services is not normally required for system functionality. It is recommended to disable the service to reduce the potential attach surface.
2.2.4 Ensure CUPS is not enabled	Description

	The Common Unix Print System (CUPS) provides the ability to print to both local and network printers. A system running CUPS can also accept print jobs from remote systems and print them to local printers. It also provides a web based remote administration capability. Rationale If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be disabled to reduce the potential attack surface.
2.2.5 Ensure DHCP Server is not enabled	Description The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses. Rationale Unless a system is specifically set up to act as a DHCP server, it is recommended that this service be deleted to reduce the potential attack surface.
2.2.6 Ensure LDAP server is not enabled	Description 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. Rationale If the system will not need to act as an LDAP server, it is recommended that the software be disabled to reduce the potential attack surface.

2.2.7 Ensure NFS and RPC are not enabled	Description The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. It provides the ability for systems to mount file systems of other servers through the network. Rationale If the system does not export NFS shares or act as an NFS client, it is recommended that these services be disabled to reduce remote attack surface.
2.2.8 Ensure DNS Server is not enabled	Description The Domain Name System (DNS) is a hierarchical naming system that maps names to IP addresses for computers, services and other resources connected to a network. Rationale Unless a system is specifically designated to act as a DNS server, it is recommended that the package be deleted to reduce the potential attack surface.
2.2.9 Ensure FTP Server is not enabled	Description The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files. Rationale

	FTP does not protect the confidentiality of data or authentication credentials. It is recommended sftp be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the package be deleted to reduce the potential attack surface.
2.2.10 Ensure HTTP server is not enabled	Description HTTP or web servers provide the ability to host web site content. Rationale Unless there is a need to run the system as a web server, it is recommended that the package be deleted to reduce the potential attack surface.
2.2.11 Ensure IMAP and POP3 server is not enabled	Description dovecot is an open source IMAP and POP3 server for Linux based systems. Rationale Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the service be deleted to reduce the potential attack surface.
2.2.12 Ensure Samba is not enabled	Description The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Small

	Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems. Rationale If there is no need to mount directories and file systems to Windows systems, then this service can be deleted to reduce the potential attack surface.
2.2.13 Ensure HTTP Proxy Server is not enabled	Description Squid is a standard proxy server used in many distributions and environments. Rationale If there is no need for a proxy server, it is recommended that the squid proxy be deleted to reduce the potential attack surface.
2.2.14 Ensure SNMP Server is not enabled	Description The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system. Rationale The SNMP server communicates using SNMP v1, which transmits data in the clear and does not require authentication to execute commands. Unless absolutely necessary, it is recommended that the SNMP service not be used.

2.2.15 Ensure mail transfer agent is configured for local-only mode	Description 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. Rationale 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.
2.2.16 Ensure rsync service is not enabled	Description The rsyncd service can be used to synchronize files between systems over network links. Rationale The rsyncd service presents a security risk as it uses unencrypted protocols for communication.
2.2.17 Ensure NIS Server is not enabled	Description The Network Information Service (NIS) (formally known as Yellow Pages) is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of configuration files.

	Rationale 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 been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be disabled and other, more secure services be used
2.2.1.1 Ensure time synchronization is in use	Description 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. Rationale 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.
2.2.1.2 Ensure ntp is configured	Description 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.

	This recommendation only applies if ntp is in use on the system. Rationale If ntp is in use on the system proper configuration is vital to ensuring time synchronization is working properly.
2.2.1.3 Ensure chrony is configured	Description 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. Rationale If chrony is in use on the system proper configuration is vital to ensuring time synchronization is working properly. This recommendation only applies if chrony is in use on the system.

2.3.1 Ensure NIS Client is not installed	Description 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 (ypbind) was used to bind a machine to an NIS server and receive the distributed configuration files. Rationale 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.
2.3.2 Ensure rsh client is not installed	Description The rsh package contains the client commands for the rsh services. Rationale 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.
2.3.3 Ensure talk client is not installed	Description 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. Rationale The software presents a security risk as it uses unencrypted protocols for communication.
2.3.5 Ensure LDAP client is not installed	Description 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. Rationale 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.
3.1.1 Ensure IP forwarding is disabled	Description The net.ipv4.ip_forward flag is used to tell the system whether it can forward packets or not. Rationale Setting the flag 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.
3.2.1 Ensure source routed packets are not accepted	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 and net.ipv4.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.
3.2.2 Ensure ICMP redirects are not accepted	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 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.
3.2.5 Ensure broadcast ICMP requests are ignored	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.
3.2.6 Ensure bogus ICMP responses are ignored	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.

3.2.7 Ensure Reverse Path Filtering is enabled	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.
3.3.2 Ensure IPv6 redirects are not accepted	Description This setting prevents the system from accepting ICMP redirects. ICMP redirects tell the system about alternate routes for sending traffic. Rationale It is recommended that systems not accept ICMP redirects 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.
3.4.1 Ensure TCP Wrappers is installed	Description

	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. Rationale 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.
3.4.2 Ensure /etc/hosts.allow is configured	Description 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. Rationale The /etc/hosts.allow file supports access control by IP and helps ensure that only authorized systems can connect to the system.
3.4.4 Ensure permissions on /etc/hosts.allow are configured	Description The /etc/hosts.allow file contains networking information that is used by many applications and therefore must be readable for these applications to operate. Rationale 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.
3.4.5 Ensure permissions on /etc/hosts.deny are 644	Description 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. Rationale 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.
3.6.1 Ensure iptables is installed	Description 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. Rationale iptables is required for firewall management and configuration.
4.2.3 Ensure rsyslog or syslog-ng is installed	Description 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. Rationale 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.
4.2.1.1 Ensure rsyslog Service is enabled	Description Once the rsyslog package is installed it needs to be activated. Rationale If the rsyslog service is not activated the system may default to the syslogd service or lack logging instead.
4.2.1.3 Ensure rsyslog default file permissions configured	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.

4.2.2.1 Ensure syslog-ng service is enabled	Description Once the syslog-ng package is installed it needs to be activated. Rationale If the syslog-ng service is not activated the system may default to the syslogd service or lack logging instead.
4.2.2.3 Ensure syslog-ng default file permissions configured	Description 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. Rationale 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.
5.1.1 Ensure cron daemon is enabled	Description The cron daemon is used to execute batch jobs on the system. Rationale While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and cron is used to execute them.

5.2.2 Ensure SSH Protocol is set to 2	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.
5.2.3 Ensure SSH LogLevel is set to INFO	Description The INFO parameter specifies that login and logout activity will be logged. 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. 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.
5.2.6 Ensure SSH IgnoreRhosts is enabled	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.
5.2.7 Ensure SSH HostbasedAuthentication is disabled	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 .
5.2.9 Ensure SSH PermitEmptyPasswords is disabled	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
5.3.4 Ensure password hashing algorithm is SHA-512	Description

	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. Rationale 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. Note that these change only apply to accounts configured on the local system.
5.4.3 Ensure default group for the root account is GID 0	Description 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. Rationale Using GID 0 for the root account helps prevent root -owned files from accidentally becoming accessible to non-privileged users.
5.4.1.3 Ensure password expiration warning days is 7 or more	Description The PASS_WARN_AGE parameter in /etc/login.defs allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the PASS_WARN_AGE parameter be set to 7 or more days.

	Rationale Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.
5.4.1.5 Ensure all users last password change date is in the past	Description All users should have a password change date in the past. Rationale If a users recorded password change date is in the future then they could bypass any set password expiration.
6.1.2 Ensure permissions on /etc/passwd are configured	Description 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. Rationale 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.
6.1.3 Ensure permissions on /etc/shadow are configured	Description

	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. Rationale 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.
6.1.4 Ensure permissions on /etc/group are configured	Description 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. Rationale 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.
6.1.5 Ensure permissions on /etc/gshadow are configured	Description 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. Rationale

	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.
6.1.6 Ensure permissions on /etc/passwd- are configured	Description The /etc/passwd- file contains backup user account information. Rationale 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.
6.1.7 Ensure permissions on /etc/shadow- are configured	Description 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. Rationale 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.

6.1.8 Ensure permissions on /etc/group- are configured	Description The /etc/group- file contains a backup list of all the valid groups defined in the system. Rationale 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.
6.1.9 Ensure permissions on /etc/gshadow- are configured	Description 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. Rationale 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.
6.1.10 Ensure no world writable files exist	Description Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the chmod(2) man page for more information. Rationale

	Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.
6.2.1 Ensure password fields are not empty	Description An account with an empty password field means that anybody may log in as that user without providing a password. Rationale All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.
6.2.2 Ensure no legacy "+" entries exist in /etc/passwd	Description 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. Rationale These entries may provide an avenue for attackers to gain privileged access on the system.
6.2.3 Ensure no legacy "+" entries exist in /etc/shadow	Description 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. Rationale These entries may provide an avenue for attackers to gain privileged access on the system.
6.2.4 Ensure no legacy "+" entries exist in /etc/group	Description 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. Rationale These entries may provide an avenue for attackers to gain privileged access on the system.
6.2.5 Ensure root is the only UID 0 account	Description Any account with UID 0 has superuser privileges on the system. Rationale 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.
6.2.6 Ensure root PATH Integrity	Description

	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. Rationale 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.
6.2.9 Ensure users own their home directories	Description The user home directory is space defined for the particular user to set local environment variables and to store personal files. Rationale Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.
6.2.11 Ensure no users have .forward files	Description The .forward file specifies an email address to forward the user's mail to. Rationale 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.
6.2.12 Ensure no users have .netrc files	Description The .netrc file contains data for logging into a remote host for file transfers via FTP. Rationale 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.
6.2.13 Ensure users' .netrc Files are not group or world accessible	Description While the system administrator can establish secure permissions for users' .netrc files, the users can easily override these. Rationale .netrc files may contain unencrypted passwords that may be used to attack other systems.
6.2.14 Ensure no users have .rhosts files	Description While no .rhosts files are shipped by default, users can easily create them. Rationale

	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.
6.2.15 Ensure all groups in /etc/passwd exist in /etc/group	Description Over time, system administration errors and changes can lead to groups being defined in /etc/passwd but not in /etc/group. Rationale 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.
6.2.16 Ensure no duplicate UIDs exist	Description 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. Rationale Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.
6.2.17 Ensure no duplicate GIDs exist	Description 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. Rationale User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.
6.2.18 Ensure no duplicate user names exist	Description 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. Rationale 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.
6.2.19 Ensure no duplicate group names exist	Description 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. Rationale 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.
6.2.20 Ensure shadow group is empty	Description The shadow group allows system programs which require access the ability to read the /etc/shadow file. No users should be assigned to the shadow group. Rationale Any users assigned to the shadow group would be granted read access to the /etc/shadow file. If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed passwords to break them. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert additional user accounts.

5.1.2 Level 1 - Workstation

Rule	Description
1.1.3 Ensure nodev option set on /tmp partition	Description The nodev mount option specifies that the filesystem cannot contain special devices. Rationale 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.

1.1.4 Ensure nosuid option set on /tmp partition	Description The nosuid mount option specifies that the filesystem cannot contain setuid files. Rationale Since the /tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot create setuid files in /tmp.
1.1.7 Ensure nodev option set on /var/tmp partition	Description The nodev mount option specifies that the filesystem cannot contain special devices. Rationale 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.
1.1.8 Ensure nosuid option set on /var/tmp partition	Description The nosuid mount option specifies that the filesystem cannot contain setuid files. Rationale 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.

1.1.9 Ensure noexec option set on /var/tmp partition	Description The noexec mount option specifies that the filesystem cannot contain executable binaries. Rationale 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.
1.1.13 Ensure nodev option set on /home partition	Description The nodev mount option specifies that the filesystem cannot contain special devices. Rationale 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.
1.1.14 Ensure nodev option set on /dev/shm partitiov	Description The nodev mount option specifies that the filesystem cannot contain special devices. Rationale Since the /run/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.

1.1.15 Ensure nosuid option set on /dev/shm partitionrun	Description The nosuid mount option specifies that the filesystem cannot contain setuid files. Rationale Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.
1.1.20 Ensure sticky bit is set on all world-writable directories	Description Setting the sticky bit on world writable directories prevents users from deleting or renaming files in that directory that are not owned by them. Rationale This feature prevents the ability to delete or rename files in world writable directories (such as /tmp) that are owned by another user.
1.5.2 Ensure XD/NX support is enabled	Description Recent processors in the x86 family support the ability to prevent code execution on a per memory page basis. Generically and on AMD processors, this ability is called No Execute (NX), while on Intel processors it is called Execute Disable (XD). This ability can help prevent exploitation of buffer overflow vulnerabilities and should be activated whenever possible. Extra steps must be taken to ensure that this protection is enabled, particularly on 32-bit x86 systems. Other processors, such as Itanium and POWER, have included such support since inception and the standard kernel for those platforms supports the feature.

	Rationale Enabling any feature that can protect against buffer overflow attacks enhances the security of the system.
1.5.3 Ensure address space layout randomization (ASLR) is enabled	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.
1.5.4 Ensure prelink is disabled	Description 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. Rationale 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.

1.7.2 Ensure GDM login banner is configured	Description GDM is the GNOME Display Manager which handles graphical login for GNOME based systems. 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.
1.7.1.1 Ensure message of the day is configured properly	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.
1.7.1.2 Ensure local login warning banner is configured properly	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.
1.7.1.3 Ensure remote login warning banner is configured properly	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.
1.7.1.5 Ensure permissions on /etc/issue are configured	Description

	The contents of the /etc/issue file are displayed to users prior to login for local terminals. Rationale If the /etc/issue file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.
1.7.1.6 Ensure permissions on /etc/issue.net are configured	Description The contents of the /etc/issue.net file are displayed to users prior to login for remote connections from configured services. Rationale If the /etc/issue.net file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.
2.1.10 Ensure xinetd is not enabled	Description The eXtended InterNET Daemon (xinetd) is an open source super daemon that replaced the original inetd daemon. The xinetd daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests. Rationale If there are no xinetd services required, it is recommended that the daemon be disabled.
2.2.3 Ensure Avahi Server is not enabled	Description

	Avahi is a free zeroconf implementation, including a system for multicast DNS/DNS-SD service discovery. Avahi allows programs to publish and discover services and hosts running on a local network with no specific configuration. For example, a user can plug a computer into a network and Avahi automatically finds printers to print to, files to look at and people to talk to, as well as network services running on the machine. Rationale Automatic discovery of network services is not normally required for system functionality. It is recommended to disable the service to reduce the potential attach surface.
2.2.5 Ensure DHCP Server is not enabled	Description The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses. Rationale Unless a system is specifically set up to act as a DHCP server, it is recommended that this service be deleted to reduce the potential attack surface.
2.2.6 Ensure LDAP server is not enabled	Description 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. Rationale

	If the system will not need to act as an LDAP server, it is recommended that the software be disabled to reduce the potential attack surface.
2.2.7 Ensure NFS and RPC are not enabled	Description The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. It provides the ability for systems to mount file systems of other servers through the network. Rationale If the system does not export NFS shares or act as an NFS client, it is recommended that these services be disabled to reduce remote attack surface.
2.2.8 Ensure DNS Server is not enabled	Description The Domain Name System (DNS) is a hierarchical naming system that maps names to IP addresses for computers, services and other resources connected to a network. Rationale Unless a system is specifically designated to act as a DNS server, it is recommended that the package be deleted to reduce the potential attack surface.
2.2.9 Ensure FTP Server is not enabled	Description The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files.

	Rationale FTP does not protect the confidentiality of data or authentication credentials. It is recommended sftp be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the package be deleted to reduce the potential attack surface.
2.2.10 Ensure HTTP server is not enabled	Description HTTP or web servers provide the ability to host web site content. Rationale Unless there is a need to run the system as a web server, it is recommended that the package be deleted to reduce the potential attack surface.
2.2.11 Ensure IMAP and POP3 server is not enabled	Description dovecot is an open source IMAP and POP3 server for Linux based systems. Rationale Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the service be deleted to reduce the potential attack surface.
2.2.12 Ensure Samba is not enabled	Description

	The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Small Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems. Rationale If there is no need to mount directories and file systems to Windows systems, then this service can be deleted to reduce the potential attack surface.
2.2.13 Ensure HTTP Proxy Server is not enabled	Description Squid is a standard proxy server used in many distributions and environments. Rationale If there is no need for a proxy server, it is recommended that the squid proxy be deleted to reduce the potential attack surface.
2.2.14 Ensure SNMP Server is not enabled	Description The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system. Rationale

	The SNMP server communicates using SNMP v1, which transmits data in the clear and does not require authentication to execute commands. Unless absolutely necessary, it is recommended that the SNMP service not be used.
2.2.15 Ensure mail transfer agent is configured for local-only mode	Description 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. Rationale 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.
2.2.16 Ensure rsync service is not enabled	Description The rsyncd service can be used to synchronize files between systems over network links. Rationale The rsyncd service presents a security risk as it uses unencrypted protocols for communication.
2.2.17 Ensure NIS Server is not enabled	Description

	The Network Information Service (NIS) (formally known as Yellow Pages) is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of configuration files. Rationale 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 been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be disabled and other, more secure services be used
2.2.1.1 Ensure time synchronization is in use	Description 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. Rationale 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.
2.2.1.2 Ensure ntp is configured	Description 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. This recommendation only applies if ntp is in use on the system. Rationale If ntp is in use on the system proper configuration is vital to ensuring time synchronization is working properly.
2.2.1.3 Ensure chrony is configured	Description 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. Rationale If chrony is in use on the system proper configuration is vital to ensuring time synchronization is working properly.

	This recommendation only applies if chrony is in use on the system.
2.3.1 Ensure NIS Client is not installed	Description 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 (ypbind) was used to bind a machine to an NIS server and receive the distributed configuration files. Rationale 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.
2.3.2 Ensure rsh client is not installed	Description The rsh package contains the client commands for the rsh services. Rationale 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.

2.3.3 Ensure talk client is not installed	Description 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. Rationale The software presents a security risk as it uses unencrypted protocols for communication.
2.3.5 Ensure LDAP client is not installed	Description 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. Rationale 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.
3.1.1 Ensure IP forwarding is disabled	Description The net.ipv4.ip_forward flag is used to tell the system whether it can forward packets or not. Rationale Setting the flag 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.

3.2.1 Ensure source routed packets are not accepted	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 and net.ipv4.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.
3.2.2 Ensure ICMP redirects are not accepted	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 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.
3.2.5 Ensure broadcast ICMP requests are ignored	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.
3.2.6 Ensure bogus ICMP responses are ignored	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.
3.2.7 Ensure Reverse Path Filtering is enabled	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.
3.3.2 Ensure IPv6 redirects are not accepted	Description This setting prevents the system from accepting ICMP redirects. ICMP redirects tell the system about alternate routes for sending traffic. Rationale It is recommended that systems not accept ICMP redirects 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.

3.4.1 Ensure TCP Wrappers is installed	Description 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. Rationale 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.
3.4.2 Ensure /etc/hosts.allow is configured	Description 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. Rationale The /etc/hosts.allow file supports access control by IP and helps ensure that only authorized systems can connect to the system.
3.4.4 Ensure permissions on /etc/hosts.allow are configured	Description The /etc/hosts.allow file contains networking information that is used by many applications and therefore must be readable for these applications to operate.

	Rationale 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.
3.4.5 Ensure permissions on /etc/hosts.deny are 644	Description 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. Rationale 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.
3.6.1 Ensure iptables is installed	Description 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. Rationale iptables is required for firewall management and configuration.
4.2.3 Ensure rsyslog or syslog-ng is installed	Description

	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. Rationale 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.
4.2.1.1 Ensure rsyslog Service is enabled	Description Once the rsyslog package is installed it needs to be activated. Rationale If the rsyslog service is not activated the system may default to the syslogd service or lack logging instead.
4.2.1.3 Ensure rsyslog default file permissions configured	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.
4.2.2.1 Ensure syslog-ng service is enabled	Description Once the syslog-ng package is installed it needs to be activated. Rationale If the syslog-ng service is not activated the system may default to the syslogd service or lack logging instead.
4.2.2.3 Ensure syslog-ng default file permissions configured	Description 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. Rationale 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.
5.1.1 Ensure cron daemon is enabled	Description The cron daemon is used to execute batch jobs on the system. Rationale

	While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and cron is used to execute them.
5.2.2 Ensure SSH Protocol is set to 2	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.
5.2.3 Ensure SSH LogLevel is set to INFO	Description The INFO parameter specifies that login and logout activity will be logged. 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. 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.
5.2.6 Ensure SSH IgnoreRhosts is enabled	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.
5.2.7 Ensure SSH HostbasedAuthentication is disabled	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 .
5.2.9 Ensure SSH PermitEmptyPasswords is disabled	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

5.3.4 Ensure password hashing algorithm is SHA-512	Description 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. Rationale 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. Note that these change only apply to accounts configured on the local system.
5.4.3 Ensure default group for the root account is GID 0	Description 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. Rationale Using GID 0 for the root account helps prevent root -owned files from accidentally becoming accessible to non-privileged users.
5.4.1.3 Ensure password expiration warning days is 7 or more	Description The PASS_WARN_AGE parameter in /etc/login.defs allows an administrator to notify users that their

	password will expire in a defined number of days. It is recommended that the PASS_WARN_AGE parameter be set to 7 or more days. Rationale Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.
5.4.1.5 Ensure all users last password change date is in the past	Description All users should have a password change date in the past. Rationale If a users recorded password change date is in the future then they could bypass any set password expiration.
6.1.2 Ensure permissions on /etc/passwd are configured	Description 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. Rationale 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.

6.1.3 Ensure permissions on /etc/shadow are configured	Description 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. Rationale 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.
6.1.4 Ensure permissions on /etc/group are configured	Description 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. Rationale 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.
6.1.5 Ensure permissions on /etc/gshadow are configured	Description 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.

	Rationale 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.
6.1.6 Ensure permissions on /etc/passwd- are configured	Description The /etc/passwd- file contains backup user account information. Rationale 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.
6.1.7 Ensure permissions on /etc/shadow- are configured	Description 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. Rationale 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.
6.1.8 Ensure permissions on /etc/group- are configured	Description The /etc/group- file contains a backup list of all the valid groups defined in the system. Rationale 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.
6.1.9 Ensure permissions on /etc/gshadow- are configured	Description 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. Rationale 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.
6.1.10 Ensure no world writable files exist	Description Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the chmod(2) man page for more information.

	Rationale Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.
6.2.1 Ensure password fields are not empty	Description An account with an empty password field means that anybody may log in as that user without providing a password. Rationale All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.
6.2.2 Ensure no legacy "+" entries exist in /etc/passwd	Description 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. Rationale These entries may provide an avenue for attackers to gain privileged access on the system.
6.2.3 Ensure no legacy "+" entries exist in /etc/shadow	Description

	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. Rationale These entries may provide an avenue for attackers to gain privileged access on the system.
6.2.4 Ensure no legacy "+" entries exist in /etc/group	Description 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. Rationale These entries may provide an avenue for attackers to gain privileged access on the system.
6.2.5 Ensure root is the only UID 0 account	Description Any account with UID 0 has superuser privileges on the system. Rationale 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.

6.2.6 Ensure root PATH Integrity	Description 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. Rationale 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.
6.2.9 Ensure users own their home directories	Description The user home directory is space defined for the particular user to set local environment variables and to store personal files. Rationale Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.
6.2.11 Ensure no users have .forward files	Description The .forward file specifies an email address to forward the user's mail to. Rationale

	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.
6.2.12 Ensure no users have .netrc files	Description The .netrc file contains data for logging into a remote host for file transfers via FTP. Rationale 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.
6.2.13 Ensure users' .netrc Files are not group or world accessible	Description While the system administrator can establish secure permissions for users' .netrc files, the users can easily override these. Rationale .netrc files may contain unencrypted passwords that may be used to attack other systems.
6.2.14 Ensure no users have .rhosts files	Description While no .rhosts files are shipped by default, users can easily create them.

	Rationale 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.
6.2.15 Ensure all groups in /etc/passwd exist in /etc/group	Description Over time, system administration errors and changes can lead to groups being defined in /etc/passwd but not in /etc/group. Rationale 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.
6.2.16 Ensure no duplicate UIDs exist	Description 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. Rationale Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.
6.2.17 Ensure no duplicate GIDs exist	Description

	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. Rationale User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.
6.2.18 Ensure no duplicate user names exist	Description 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. Rationale 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.
6.2.19 Ensure no duplicate group names exist	Description 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. Rationale

	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.
6.2.20 Ensure shadow group is empty	Description The shadow group allows system programs which require access the ability to read the /etc/shadow file. No users should be assigned to the shadow group. Rationale Any users assigned to the shadow group would be granted read access to the /etc/shadow file. If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed passwords to break them. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert additional user accounts.

5.1.3 Level 2 - Server

Rule	Description
1.1.3 Ensure nodev option set on /tmp partition	Description The nodev mount option specifies that the filesystem cannot contain special devices. Rationale 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.

1.1.4 Ensure nosuid option set on /tmp partition	Description The nosuid mount option specifies that the filesystem cannot contain setuid files. Rationale Since the /tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot create setuid files in /tmp.
1.1.7 Ensure nodev option set on /var/tmp partition	Description The nodev mount option specifies that the filesystem cannot contain special devices. Rationale 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.
1.1.8 Ensure nosuid option set on /var/tmp partition	Description The nosuid mount option specifies that the filesystem cannot contain setuid files. Rationale 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.

1.1.9 Ensure noexec option set on /var/tmp partition	Description The noexec mount option specifies that the filesystem cannot contain executable binaries. Rationale 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.
1.1.13 Ensure nodev option set on /home partition	Description The nodev mount option specifies that the filesystem cannot contain special devices. Rationale 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.
1.1.14 Ensure nodev option set on /dev/shm partitiov	Description The nodev mount option specifies that the filesystem cannot contain special devices. Rationale Since the /run/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.

1.1.15 Ensure nosuid option set on /dev/shm partitionrun	Description The nosuid mount option specifies that the filesystem cannot contain setuid files. Rationale Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.
1.1.20 Ensure sticky bit is set on all world-writable directories	Description Setting the sticky bit on world writable directories prevents users from deleting or renaming files in that directory that are not owned by them. Rationale This feature prevents the ability to delete or rename files in world writable directories (such as /tmp) that are owned by another user.
1.1.21 Disable Automounting	Description autofs allows automatic mounting of devices, typically including CD/DVDs and USB drives. Rationale With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.

1.5.2 Ensure XD/NX support is enabled	Description Recent processors in the x86 family support the ability to prevent code execution on a per memory page basis. Generically and on AMD processors, this ability is called No Execute (NX), while on Intel processors it is called Execute Disable (XD). This ability can help prevent exploitation of buffer overflow vulnerabilities and should be activated whenever possible. Extra steps must be taken to ensure that this protection is enabled, particularly on 32-bit x86 systems. Other processors, such as Itanium and POWER, have included such support since inception and the standard kernel for those platforms supports the feature. Rationale Enabling any feature that can protect against buffer overflow attacks enhances the security of the system.
1.5.3 Ensure address space layout randomization (ASLR) is enabled	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.
1.5.4 Ensure prelink is disabled	Description

	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. Rationale 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.
1.6.3 Ensure SELinux or AppArmor are installed	Description SELinux and AppArmor provide Mandatory Access Controls. Rationale Without a Mandatory Access Control system installed only the default Discretionary Access Control system will be available.
1.6.1.1 Ensure SELinux is not disabled in bootloader configuration	Description Configure SELINUX to be enabled at boot time and verify that it has not been overwritten by the grub boot parameters. Rationale SELinux must be enabled at boot time in your grub configuration to ensure that the controls it provides are not overridden.

1.6.1.2 Ensure the SELinux state is enforcing	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.
1.6.1.3 Ensure SELinux policy is configured	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.
1.6.1.4 Ensure no unconfined daemons exist	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.

1.6.2.1 Ensure AppArmor is not disabled in bootloader configuration	Description Configure AppArmor to be enabled at boot time and verify that it has not been overwritten by the bootloader boot parameters. Rationale AppArmor must be enabled at boot time in your bootloader configuration to ensure that the controls it provides are not overridden.
1.7.2 Ensure GDM login banner is configured	Description GDM is the GNOME Display Manager which handles graphical login for GNOME based systems. 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.
1.7.1.1 Ensure message of the day is configured properly	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.
1.7.1.2 Ensure local login warning banner is configured properly	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.
1.7.1.3 Ensure remote login warning banner is configured properly	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.
1.7.1.5 Ensure permissions on /etc/issue are configured	Description The contents of the /etc/issue file are displayed to users prior to login for local terminals. Rationale If the /etc/issue file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.
1.7.1.6 Ensure permissions on /etc/issue.net are configured	Description The contents of the /etc/issue.net file are displayed to users prior to login for remote connections from configured services. Rationale If the /etc/issue.net file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.

2.1.10 Ensure xinetd is not enabled	Description The eXtended InterNET Daemon (xinetd) is an open source super daemon that replaced the original inetd daemon. The xinetd daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests. Rationale If there are no xinetd services required, it is recommended that the daemon be disabled.
2.2.2 Ensure X Window System is not installed	Description 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. Rationale Unless your organization specifically requires graphical login access via X Windows, remove it to reduce the potential attack surface.
2.2.3 Ensure Avahi Server is not enabled	Description Avahi is a free zeroconf implementation, including a system for multicast DNS/DNS-SD service discovery. Avahi allows programs to publish and discover services and hosts running on a local network with no specific configuration. For example, a user can plug a computer into a network and Avahi automatically finds printers to print to, files to look at and people to talk to, as well as network services running on the machine.

	Rationale Automatic discovery of network services is not normally required for system functionality. It is recommended to disable the service to reduce the potential attach surface.
2.2.4 Ensure CUPS is not enabled	Description The Common Unix Print System (CUPS) provides the ability to print to both local and network printers. A system running CUPS can also accept print jobs from remote systems and print them to local printers. It also provides a web based remote administration capability. Rationale If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be disabled to reduce the potential attack surface.
2.2.5 Ensure DHCP Server is not enabled	Description The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses. Rationale Unless a system is specifically set up to act as a DHCP server, it is recommended that this service be deleted to reduce the potential attack surface.
2.2.6 Ensure LDAP server is not enabled	Description

	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. Rationale If the system will not need to act as an LDAP server, it is recommended that the software be disabled to reduce the potential attack surface.
2.2.7 Ensure NFS and RPC are not enabled	Description The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. It provides the ability for systems to mount file systems of other servers through the network. Rationale If the system does not export NFS shares or act as an NFS client, it is recommended that these services be disabled to reduce remote attack surface.
2.2.8 Ensure DNS Server is not enabled	Description The Domain Name System (DNS) is a hierarchical naming system that maps names to IP addresses for computers, services and other resources connected to a network. Rationale

	Unless a system is specifically designated to act as a DNS server, it is recommended that the package be deleted to reduce the potential attack surface.
2.2.9 Ensure FTP Server is not enabled	Description The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files. Rationale FTP does not protect the confidentiality of data or authentication credentials. It is recommended sftp be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the package be deleted to reduce the potential attack surface.
2.2.10 Ensure HTTP server is not enabled	Description HTTP or web servers provide the ability to host web site content. Rationale Unless there is a need to run the system as a web server, it is recommended that the package be deleted to reduce the potential attack surface.
2.2.11 Ensure IMAP and POP3 server is not enabled	Description dovecot is an open source IMAP and POP3 server for Linux based systems.

	Rationale Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the service be deleted to reduce the potential attack surface.
2.2.12 Ensure Samba is not enabled	Description The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Small Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems. Rationale If there is no need to mount directories and file systems to Windows systems, then this service can be deleted to reduce the potential attack surface.
2.2.13 Ensure HTTP Proxy Server is not enabled	Description Squid is a standard proxy server used in many distributions and environments. Rationale If there is no need for a proxy server, it is recommended that the squid proxy be deleted to reduce the potential attack surface.
2.2.14 Ensure SNMP Server is not enabled	Description

	The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system. Rationale The SNMP server communicates using SNMP v1, which transmits data in the clear and does not require authentication to execute commands. Unless absolutely necessary, it is recommended that the SNMP service not be used.
2.2.15 Ensure mail transfer agent is configured for local-only mode	Description 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. Rationale 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.
2.2.16 Ensure rsync service is not enabled	Description The rsyncd service can be used to synchronize files between systems over network links.

	Rationale The rsyncd service presents a security risk as it uses unencrypted protocols for communication.
2.2.17 Ensure NIS Server is not enabled	Description The Network Information Service (NIS) (formally known as Yellow Pages) is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of configuration files. Rationale 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 been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be disabled and other, more secure services be used
2.2.1.1 Ensure time synchronization is in use	Description 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. Rationale 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.

2.2.1.2 Ensure ntp is configured	Description 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. This recommendation only applies if ntp is in use on the system. Rationale If ntp is in use on the system proper configuration is vital to ensuring time synchronization is working properly.
2.2.1.3 Ensure chrony is configured	Description 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.

	Rationale If chrony is in use on the system proper configuration is vital to ensuring time synchronization is working properly. This recommendation only applies if chrony is in use on the system.
2.3.1 Ensure NIS Client is not installed	Description 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 (ypbind) was used to bind a machine to an NIS server and receive the distributed configuration files. Rationale 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.
2.3.2 Ensure rsh client is not installed	Description The rsh package contains the client commands for the rsh services. Rationale

	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.
2.3.3 Ensure talk client is not installed	Description 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. Rationale The software presents a security risk as it uses unencrypted protocols for communication.
2.3.5 Ensure LDAP client is not installed	Description 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. Rationale 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.
3.1.1 Ensure IP forwarding is disabled	Description

	The net.ipv4.ip_forward flag is used to tell the system whether it can forward packets or not. Rationale Setting the flag 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.
3.2.1 Ensure source routed packets are not accepted	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 and net.ipv4.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.
3.2.2 Ensure ICMP redirects are not accepted	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 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.
3.2.5 Ensure broadcast ICMP requests are ignored	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.
3.2.6 Ensure bogus ICMP responses are ignored	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.
3.2.7 Ensure Reverse Path Filtering is enabled	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.
3.3.2 Ensure IPv6 redirects are not accepted	Description This setting prevents the system from accepting ICMP redirects. ICMP redirects tell the system about alternate routes for sending traffic.

	Rationale It is recommended that systems not accept ICMP redirects 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.
3.4.1 Ensure TCP Wrappers is installed	Description 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. Rationale 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.
3.4.2 Ensure /etc/hosts.allow is configured	Description 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. Rationale The /etc/hosts.allow file supports access control by IP and helps ensure that only authorized systems can connect to the system.

3.4.4 Ensure permissions on /etc/hosts.allow are configured	Description The /etc/hosts.allow file contains networking information that is used by many applications and therefore must be readable for these applications to operate. Rationale 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.
3.4.5 Ensure permissions on /etc/hosts.deny are 644	Description 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. Rationale 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.
3.6.1 Ensure iptables is installed	Description 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.

	Rationale iptables is required for firewall management and configuration.
4.1.12 Ensure use of privileged commands is collected	Description Monitor privileged programs (those that have the setuid and/or setgid bit set on execution) to determine if unprivileged users are running these commands. Rationale Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.
4.2.3 Ensure rsyslog or syslog-ng is installed	Description 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. Rationale 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.

4.2.1.1 Ensure rsyslog Service is enabled	Description Once the rsyslog package is installed it needs to be activated. Rationale If the rsyslog service is not activated the system may default to the syslogd service or lack logging instead.
4.2.1.3 Ensure rsyslog default file permissions configured	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.
4.2.2.1 Ensure syslog-ng service is enabled	Description Once the syslog-ng package is installed it needs to be activated. Rationale If the syslog-ng service is not activated the system may default to the syslogd service or lack logging instead.

4.2.2.3 Ensure syslog-ng default file permissions configured	Description 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. Rationale 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.
5.1.1 Ensure cron daemon is enabled	Description The cron daemon is used to execute batch jobs on the system. Rationale While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and cron is used to execute them.
5.2.2 Ensure SSH Protocol is set to 2	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.

5.2.3 Ensure SSH LogLevel is set to INFO	Description The INFO parameter specifies that login and logout activity will be logged. 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. 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.
5.2.6 Ensure SSH IgnoreRhosts is enabled	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.
5.2.7 Ensure SSH HostbasedAuthentication is disabled	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 .
5.2.9 Ensure SSH PermitEmptyPasswords is disabled	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
5.3.4 Ensure password hashing algorithm is SHA-512	Description 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. Rationale 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.

	Note that these change only apply to accounts configured on the local system.
5.4.3 Ensure default group for the root account is GID 0	Description 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. Rationale Using GID 0 for the root account helps prevent root -owned files from accidentally becoming accessible to non-privileged users.
5.4.1.3 Ensure password expiration warning days is 7 or more	Description The PASS_WARN_AGE parameter in /etc/login.defs allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the PASS_WARN_AGE parameter be set to 7 or more days. Rationale Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.
5.4.1.5 Ensure all users last password change date is in the past	Description All users should have a password change date in the past.

	Rationale If a users recorded password change date is in the future then they could bypass any set password expiration.
6.1.2 Ensure permissions on /etc/passwd are configured	Description 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. Rationale 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.
6.1.3 Ensure permissions on /etc/shadow are configured	Description 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. Rationale 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.

6.1.4 Ensure permissions on /etc/group are configured	Description 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. Rationale 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.
6.1.5 Ensure permissions on /etc/gshadow are configured	Description 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. Rationale 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.
6.1.6 Ensure permissions on /etc/passwd- are configured	Description The /etc/passwd- file contains backup user account information. Rationale

	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.
6.1.7 Ensure permissions on /etc/shadow- are configured	Description 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. Rationale 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.
6.1.8 Ensure permissions on /etc/group- are configured	Description The /etc/group- file contains a backup list of all the valid groups defined in the system. Rationale 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.

6.1.9 Ensure permissions on /etc/gshadow- are configured	Description 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. Rationale 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.
6.1.10 Ensure no world writable files exist	Description Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the chmod(2) man page for more information. Rationale Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written script or program that could potentially be the cause of a larger compromise to the system's integrity.
6.2.1 Ensure password fields are not empty	Description An account with an empty password field means that anybody may log in as that user without providing a password. Rationale

	All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.
6.2.2 Ensure no legacy "+" entries exist in /etc/passwd	Description 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. Rationale These entries may provide an avenue for attackers to gain privileged access on the system.
6.2.3 Ensure no legacy "+" entries exist in /etc/shadow	Description 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. Rationale These entries may provide an avenue for attackers to gain privileged access on the system.
6.2.4 Ensure no legacy "+" entries exist in /etc/group	Description 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. Rationale These entries may provide an avenue for attackers to gain privileged access on the system.
6.2.5 Ensure root is the only UID 0 account	Description Any account with UID 0 has superuser privileges on the system. Rationale 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.
6.2.6 Ensure root PATH Integrity	Description 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. Rationale 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.

6.2.9 Ensure users own their home directories	Description The user home directory is space defined for the particular user to set local environment variables and to store personal files. Rationale Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.
6.2.11 Ensure no users have .forward files	Description The .forward file specifies an email address to forward the user's mail to. Rationale 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.
6.2.12 Ensure no users have .netrc files	Description The .netrc file contains data for logging into a remote host for file transfers via FTP. Rationale 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.
6.2.13 Ensure users' .netrc Files are not group or world accessible	Description While the system administrator can establish secure permissions for users' .netrc files, the users can easily override these. Rationale .netrc files may contain unencrypted passwords that may be used to attack other systems.
6.2.14 Ensure no users have .rhosts files	Description While no .rhosts files are shipped by default, users can easily create them. Rationale 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.
6.2.15 Ensure all groups in /etc/passwd exist in /etc/group	Description Over time, system administration errors and changes can lead to groups being defined in /etc/passwd but not in /etc/group.

	Rationale 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.
6.2.16 Ensure no duplicate UIDs exist	Description 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. Rationale Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.
6.2.17 Ensure no duplicate GIDs exist	Description 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. Rationale User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.
6.2.18 Ensure no duplicate user names exist	Description 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. Rationale 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.
6.2.19 Ensure no duplicate group names exist	Description 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. Rationale 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.
6.2.20 Ensure shadow group is empty	Description The shadow group allows system programs which require access the ability to read the /etc/shadow file. No users should be assigned to the shadow group. Rationale Any users assigned to the shadow group would be granted read access to the /etc/shadow file. If attackers

	can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed passwords to break them. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert additional user accounts.

5.1.4 Level 2 - Workstation

Rule	Description
1.1.3 Ensure nodev option set on /tmp partition	Description The nodev mount option specifies that the filesystem cannot contain special devices. Rationale 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.
1.1.4 Ensure nosuid option set on /tmp partition	Description The nosuid mount option specifies that the filesystem cannot contain setuid files. Rationale Since the /tmp filesystem is only intended for temporary file storage, set this option to ensure that users cannot create setuid files in /tmp.
1.1.7 Ensure nodev option set on /var/tmp partition	Description

	The nodev mount option specifies that the filesystem cannot contain special devices. Rationale 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.
1.1.8 Ensure nosuid option set on /var/tmp partition	Description The nosuid mount option specifies that the filesystem cannot contain setuid files. Rationale 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.
1.1.9 Ensure noexec option set on /var/tmp partition	Description The noexec mount option specifies that the filesystem cannot contain executable binaries. Rationale 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.
1.1.13 Ensure nodev option set on /home partition	Description

	The nodev mount option specifies that the filesystem cannot contain special devices. Rationale 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.
1.1.14 Ensure nodev option set on /dev/shm partitiov	Description The nodev mount option specifies that the filesystem cannot contain special devices. Rationale Since the /run/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.
1.1.15 Ensure nosuid option set on /dev/shm partitionrun	Description The nosuid mount option specifies that the filesystem cannot contain setuid files. Rationale Setting this option on a file system prevents users from introducing privileged programs onto the system and allowing non-root users to execute them.
1.1.20 Ensure sticky bit is set on all world-writable directories	Description

	Setting the sticky bit on world writable directories prevents users from deleting or renaming files in that directory that are not owned by them. Rationale This feature prevents the ability to delete or rename files in world writable directories (such as /tmp) that are owned by another user.
1.1.21 Disable Automounting	Description autofs allows automatic mounting of devices, typically including CD/DVDs and USB drives. Rationale With automounting enabled anyone with physical access could attach a USB drive or disc and have its contents available in system even if they lacked permissions to mount it themselves.
1.5.2 Ensure XD/NX support is enabled	Description Recent processors in the x86 family support the ability to prevent code execution on a per memory page basis. Generically and on AMD processors, this ability is called No Execute (NX), while on Intel processors it is called Execute Disable (XD). This ability can help prevent exploitation of buffer overflow vulnerabilities and should be activated whenever possible. Extra steps must be taken to ensure that this protection is enabled, particularly on 32-bit x86 systems. Other processors, such as Itanium and POWER, have included such support since inception and the standard kernel for those platforms supports the feature.

	Rationale Enabling any feature that can protect against buffer overflow attacks enhances the security of the system.
1.5.3 Ensure address space layout randomization (ASLR) is enabled	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.
1.5.4 Ensure prelink is disabled	Description 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. Rationale 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.
1.6.3 Ensure SELinux or AppArmor are installed	Description

	SELinux and AppArmor provide Mandatory Access Controls. Rationale Without a Mandatory Access Control system installed only the default Discretionary Access Control system will be available.
1.6.1.1 Ensure SELinux is not disabled in bootloader configuration	Description Configure SELINUX to be enabled at boot time and verify that it has not been overwritten by the grub boot parameters. Rationale SELinux must be enabled at boot time in your grub configuration to ensure that the controls it provides are not overridden.
1.6.1.2 Ensure the SELinux state is enforcing	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.
1.6.1.3 Ensure SELinux policy is configured	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.
1.6.1.4 Ensure no unconfined daemons exist	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.
1.6.2.1 Ensure AppArmor is not disabled in bootloader configuration	Description Configure AppArmor to be enabled at boot time and verify that it has not been overwritten by the bootloader boot parameters. Rationale AppArmor must be enabled at boot time in your bootloader configuration to ensure that the controls it provides are not overridden.

1.7.2 Ensure GDM login banner is configured	Description GDM is the GNOME Display Manager which handles graphical login for GNOME based systems. 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.
1.7.1.1 Ensure message of the day is configured properly	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.
1.7.1.2 Ensure local login warning banner is configured properly	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.
1.7.1.3 Ensure remote login warning banner is configured properly	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.

1.7.1.5 Ensure permissions on /etc/issue are configured	Description The contents of the /etc/issue file are displayed to users prior to login for local terminals. Rationale If the /etc/issue file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.
1.7.1.6 Ensure permissions on /etc/issue.net are configured	Description The contents of the /etc/issue.net file are displayed to users prior to login for remote connections from configured services. Rationale If the /etc/issue.net file does not have the correct ownership it could be modified by unauthorized users with incorrect or misleading information.
2.1.10 Ensure xinetd is not enabled	Description The eXtended InterNET Daemon (xinetd) is an open source super daemon that replaced the original inetd daemon. The xinetd daemon listens for well known services and dispatches the appropriate daemon to properly respond to service requests. Rationale If there are no xinetd services required, it is recommended that the daemon be disabled.

2.2.3 Ensure Avahi Server is not enabled	Description Avahi is a free zeroconf implementation, including a system for multicast DNS/DNS-SD service discovery. Avahi allows programs to publish and discover services and hosts running on a local network with no specific configuration. For example, a user can plug a computer into a network and Avahi automatically finds printers to print to, files to look at and people to talk to, as well as network services running on the machine. Rationale Automatic discovery of network services is not normally required for system functionality. It is recommended to disable the service to reduce the potential attach surface.
2.2.4 Ensure CUPS is not enabled	Description The Common Unix Print System (CUPS) provides the ability to print to both local and network printers. A system running CUPS can also accept print jobs from remote systems and print them to local printers. It also provides a web based remote administration capability. Rationale If the system does not need to print jobs or accept print jobs from other systems, it is recommended that CUPS be disabled to reduce the potential attack surface.
2.2.5 Ensure DHCP Server is not enabled	Description The Dynamic Host Configuration Protocol (DHCP) is a service that allows machines to be dynamically assigned IP addresses.

	Rationale Unless a system is specifically set up to act as a DHCP server, it is recommended that this service be deleted to reduce the potential attack surface.
2.2.6 Ensure LDAP server is not enabled	Description 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. Rationale If the system will not need to act as an LDAP server, it is recommended that the software be disabled to reduce the potential attack surface.
2.2.7 Ensure NFS and RPC are not enabled	Description The Network File System (NFS) is one of the first and most widely distributed file systems in the UNIX environment. It provides the ability for systems to mount file systems of other servers through the network. Rationale If the system does not export NFS shares or act as an NFS client, it is recommended that these services be disabled to reduce remote attack surface.
2.2.8 Ensure DNS Server is not enabled	Description

	The Domain Name System (DNS) is a hierarchical naming system that maps names to IP addresses for computers, services and other resources connected to a network. Rationale Unless a system is specifically designated to act as a DNS server, it is recommended that the package be deleted to reduce the potential attack surface.
2.2.9 Ensure FTP Server is not enabled	Description The File Transfer Protocol (FTP) provides networked computers with the ability to transfer files. Rationale FTP does not protect the confidentiality of data or authentication credentials. It is recommended sftp be used if file transfer is required. Unless there is a need to run the system as a FTP server (for example, to allow anonymous downloads), it is recommended that the package be deleted to reduce the potential attack surface.
2.2.10 Ensure HTTP server is not enabled	Description HTTP or web servers provide the ability to host web site content. Rationale Unless there is a need to run the system as a web server, it is recommended that the package be deleted to reduce the potential attack surface.

2.2.11 Ensure IMAP and POP3 server is not enabled	Description dovecot is an open source IMAP and POP3 server for Linux based systems. Rationale Unless POP3 and/or IMAP servers are to be provided by this system, it is recommended that the service be deleted to reduce the potential attack surface.
2.2.12 Ensure Samba is not enabled	Description The Samba daemon allows system administrators to configure their Linux systems to share file systems and directories with Windows desktops. Samba will advertise the file systems and directories via the Small Message Block (SMB) protocol. Windows desktop users will be able to mount these directories and file systems as letter drives on their systems. Rationale If there is no need to mount directories and file systems to Windows systems, then this service can be deleted to reduce the potential attack surface.
2.2.13 Ensure HTTP Proxy Server is not enabled	Description Squid is a standard proxy server used in many distributions and environments. Rationale

	If there is no need for a proxy server, it is recommended that the squid proxy be deleted to reduce the potential attack surface.
2.2.14 Ensure SNMP Server is not enabled	Description The Simple Network Management Protocol (SNMP) server is used to listen for SNMP commands from an SNMP management system, execute the commands or collect the information and then send results back to the requesting system. Rationale The SNMP server communicates using SNMP v1, which transmits data in the clear and does not require authentication to execute commands. Unless absolutely necessary, it is recommended that the SNMP service not be used.
2.2.15 Ensure mail transfer agent is configured for local-only mode	Description 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. Rationale 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.

2.2.16 Ensure rsync service is not enabled	Description The rsyncd service can be used to synchronize files between systems over network links. Rationale The rsyncd service presents a security risk as it uses unencrypted protocols for communication.
2.2.17 Ensure NIS Server is not enabled	Description The Network Information Service (NIS) (formally known as Yellow Pages) is a client-server directory service protocol for distributing system configuration files. The NIS server is a collection of programs that allow for the distribution of configuration files. Rationale 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 been replaced by such protocols as Lightweight Directory Access Protocol (LDAP). It is recommended that the service be disabled and other, more secure services be used
2.2.1.1 Ensure time synchronization is in use	Description 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.

	Rationale 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.
2.2.1.2 Ensure ntp is configured	Description 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. This recommendation only applies if ntp is in use on the system. Rationale If ntp is in use on the system proper configuration is vital to ensuring time synchronization is working properly.
2.2.1.3 Ensure chrony is configured	Description

	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. Rationale If chrony is in use on the system proper configuration is vital to ensuring time synchronization is working properly. This recommendation only applies if chrony is in use on the system.
2.3.1 Ensure NIS Client is not installed	Description 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 (ypbind) was used to bind a machine to an NIS server and receive the distributed configuration files. Rationale 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.

2.3.2 Ensure rsh client is not installed	Description The rsh package contains the client commands for the rsh services. Rationale 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.
2.3.3 Ensure talk client is not installed	Description 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. Rationale The software presents a security risk as it uses unencrypted protocols for communication.
2.3.5 Ensure LDAP client is not installed	Description 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. Rationale

	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.
3.1.1 Ensure IP forwarding is disabled	Description The net.ipv4.ip_forward flag is used to tell the system whether it can forward packets or not. Rationale Setting the flag 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.
3.2.1 Ensure source routed packets are not accepted	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 and net.ipv4.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.
3.2.2 Ensure ICMP redirects are not accepted	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 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.
3.2.5 Ensure broadcast ICMP requests are ignored	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.
3.2.6 Ensure bogus ICMP responses are ignored	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.
3.2.7 Ensure Reverse Path Filtering is enabled	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.
3.3.2 Ensure IPv6 redirects are not accepted	Description This setting prevents the system from accepting ICMP redirects. ICMP redirects tell the system about alternate routes for sending traffic. Rationale It is recommended that systems not accept ICMP redirects 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.
3.4.1 Ensure TCP Wrappers is installed	Description 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. Rationale 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.
3.4.2 Ensure /etc/hosts.allow is configured	Description

	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. Rationale The /etc/hosts.allow file supports access control by IP and helps ensure that only authorized systems can connect to the system.
3.4.4 Ensure permissions on /etc/hosts.allow are configured	Description The /etc/hosts.allow file contains networking information that is used by many applications and therefore must be readable for these applications to operate. Rationale 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.
3.4.5 Ensure permissions on /etc/hosts.deny are 644	Description 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. Rationale 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.

3.6.1 Ensure iptables is installed	Description 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. Rationale iptables is required for firewall management and configuration.
4.1.12 Ensure use of privileged commands is collected	Description Monitor privileged programs (those that have the setuid and/or setgid bit set on execution) to determine if unprivileged users are running these commands. Rationale Execution of privileged commands by non-privileged users could be an indication of someone trying to gain unauthorized access to the system.
4.2.3 Ensure rsyslog or syslog-ng is installed	Description 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.

	Rationale 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.
4.2.1.1 Ensure rsyslog Service is enabled	Description Once the rsyslog package is installed it needs to be activated. Rationale If the rsyslog service is not activated the system may default to the syslogd service or lack logging instead.
4.2.1.3 Ensure rsyslog default file permissions configured	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.
4.2.2.1 Ensure syslog-ng service is enabled	Description

	Once the syslog-ng package is installed it needs to be activated. Rationale If the syslog-ng service is not activated the system may default to the syslogd service or lack logging instead.
4.2.2.3 Ensure syslog-ng default file permissions configured	Description 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. Rationale 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.
5.1.1 Ensure cron daemon is enabled	Description The cron daemon is used to execute batch jobs on the system. Rationale While there may not be user jobs that need to be run on the system, the system does have maintenance jobs that may include security monitoring that have to run, and cron is used to execute them.
5.2.2 Ensure SSH Protocol is set to 2	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.
5.2.3 Ensure SSH LogLevel is set to INFO	Description The INFO parameter specifies that login and logout activity will be logged. 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. 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.
5.2.6 Ensure SSH IgnoreRhosts is enabled	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.
5.2.7 Ensure SSH HostbasedAuthentication is disabled	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 .
5.2.9 Ensure SSH PermitEmptyPasswords is disabled	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
5.3.4 Ensure password hashing algorithm is SHA-512	Description 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.

	Rationale 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. Note that these change only apply to accounts configured on the local system.
5.4.3 Ensure default group for the root account is GID 0	Description 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. Rationale Using GID 0 for the root account helps prevent root -owned files from accidentally becoming accessible to non-privileged users.
5.4.1.3 Ensure password expiration warning days is 7 or more	Description The PASS_WARN_AGE parameter in /etc/login.defs allows an administrator to notify users that their password will expire in a defined number of days. It is recommended that the PASS_WARN_AGE parameter be set to 7 or more days. Rationale

	Providing an advance warning that a password will be expiring gives users time to think of a secure password. Users caught unaware may choose a simple password or write it down where it may be discovered.
5.4.1.5 Ensure all users last password change date is in the past	Description All users should have a password change date in the past. Rationale If a users recorded password change date is in the future then they could bypass any set password expiration.
6.1.2 Ensure permissions on /etc/passwd are configured	Description 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. Rationale 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.
6.1.3 Ensure permissions on /etc/shadow are configured	Description 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.

	Rationale 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.
6.1.4 Ensure permissions on /etc/group are configured	Description 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. Rationale 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.
6.1.5 Ensure permissions on /etc/gshadow are configured	Description 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. Rationale 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.
6.1.6 Ensure permissions on /etc/passwd- are configured	Description The /etc/passwd- file contains backup user account information. Rationale 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.
6.1.7 Ensure permissions on /etc/shadow- are configured	Description 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. Rationale 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.
6.1.8 Ensure permissions on /etc/group- are configured	Description

	The /etc/group- file contains a backup list of all the valid groups defined in the system. Rationale 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.
6.1.9 Ensure permissions on /etc/gshadow- are configured	Description 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. Rationale 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.
6.1.10 Ensure no world writable files exist	Description Unix-based systems support variable settings to control access to files. World writable files are the least secure. See the chmod(2) man page for more information. Rationale Data in world-writable files can be modified and compromised by any user on the system. World writable files may also indicate an incorrectly written

	script or program that could potentially be the cause of a larger compromise to the system's integrity.
6.2.1 Ensure password fields are not empty	Description An account with an empty password field means that anybody may log in as that user without providing a password. Rationale All accounts must have passwords or be locked to prevent the account from being used by an unauthorized user.
6.2.2 Ensure no legacy "+" entries exist in /etc/passwd	Description 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. Rationale These entries may provide an avenue for attackers to gain privileged access on the system.
6.2.3 Ensure no legacy "+" entries exist in /etc/shadow	Description 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.

	Rationale These entries may provide an avenue for attackers to gain privileged access on the system.
6.2.4 Ensure no legacy "+" entries exist in /etc/group	Description 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. Rationale These entries may provide an avenue for attackers to gain privileged access on the system.
6.2.5 Ensure root is the only UID 0 account	Description Any account with UID 0 has superuser privileges on the system. Rationale 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.
6.2.6 Ensure root PATH Integrity	Description

	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. Rationale 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.
6.2.9 Ensure users own their home directories	Description The user home directory is space defined for the particular user to set local environment variables and to store personal files. Rationale Since the user is accountable for files stored in the user home directory, the user must be the owner of the directory.
6.2.11 Ensure no users have .forward files	Description The .forward file specifies an email address to forward the user's mail to. Rationale 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.

6.2.12 Ensure no users have .netrc files	Description The .netrc file contains data for logging into a remote host for file transfers via FTP. Rationale 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.
6.2.13 Ensure users' .netrc Files are not group or world accessible	Description While the system administrator can establish secure permissions for users' .netrc files, the users can easily override these. Rationale .netrc files may contain unencrypted passwords that may be used to attack other systems.
6.2.14 Ensure no users have .rhosts files	Description While no .rhosts files are shipped by default, users can easily create them. Rationale 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.
6.2.15 Ensure all groups in /etc/passwd exist in /etc/group	Description Over time, system administration errors and changes can lead to groups being defined in /etc/passwd but not in /etc/group. Rationale 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.
6.2.16 Ensure no duplicate UIDs exist	Description 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. Rationale Users must be assigned unique UIDs for accountability and to ensure appropriate access protections.
6.2.17 Ensure no duplicate GIDs exist	Description 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.

	Rationale User groups must be assigned unique GIDs for accountability and to ensure appropriate access protections.
6.2.18 Ensure no duplicate user names exist	Description 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. Rationale 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.
6.2.19 Ensure no duplicate group names exist	Description 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. Rationale 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.

6.2.20 Ensure shadow group is empty	Description The shadow group allows system programs which require access the ability to read the /etc/shadow file. No users should be assigned to the shadow group. Rationale Any users assigned to the shadow group would be granted read access to the /etc/shadow file. If attackers can gain read access to the /etc/shadow file, they can easily run a password cracking program against the hashed passwords to break them. Other security information that is stored in the /etc/shadow file (such as expiration) could also be useful to subvert additional user accounts.

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/webframeloaderclient_impl.cc in Google Chrome before 3.0.195.32 allows user-assisted remote attackers to cause a denial of service via a page-local link, related to an "empty redirect chain," as demonstrated by a message in Yahoo! Mail.
CVE-2009-5072	Memory leak in the ldap_explode_dn function in IBM Tivoli Directory Server (TDS) 6.0 before 6.0.0.61 (aka 6.0.0.8-TIV-ITDS-IF0003) allows remote

	authenticated users to cause a denial of service (memory consumption) via an empty string argument.
CVE-2009-5073	IBM Tivoli Directory Server (TDS) 6.0 before 6.0.0.59 (aka 6.0.0.8-TIV-ITDS-IF0001) allows remote authenticated users to cause a denial of service (infinite loop and daemon hang) by adding a nested group that contains the Distinguished Name (DN) of its parent entry.
CVE-2010-0185	The default configuration of Adobe ColdFusion 9.0 does not restrict access to collections that have been created by the Solr Service, which allows remote attackers to obtain collection metadata, search information, and index data via a request to an unspecified URL.
CVE-2010-0186	Cross-domain vulnerability in Adobe Flash Player before 10.0.45.2, Adobe AIR before 1.5.3.9130, and Adobe Reader and Acrobat 8.x before 8.2.1 and 9.x before 9.3.1 allows remote attackers to bypass intended sandbox restrictions and make cross-domain requests via unspecified vectors.
CVE-2010-0187	Adobe Flash Player before 10.0.45.2 and Adobe AIR before 1.5.3.9130 allow remote attackers to cause a denial of service (application crash) via a modified SWF file.
CVE-2010-0190	Cross-site scripting (XSS) vulnerability in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2010-0191	Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allow attackers to execute arbitrary code via unspecified vectors, related to a "prefix protocol handler vulnerability."
CVE-2010-0192	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2010-0193 and CVE-2010-0196.
CVE-2010-0193	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2010-0192 and CVE-2010-0196.
CVE-2010-0194	Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allow attackers to cause a denial of service (memory corruption) or execute arbitrary code via unspecified

	vectors, a different vulnerability than CVE-2010-0197, CVE-2010-0201, and CVE-2010-0204.
CVE-2010-0195	Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, do not properly handle fonts, which allows attackers to execute arbitrary code via unspecified vectors.
CVE-2010-0196	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2010-0192 and CVE-2010-0193.
CVE-2010-0197	Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allow attackers to cause a denial of service (memory corruption) or execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0194, CVE-2010-0201, and CVE-2010-0204.
CVE-2010-0198	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0199, CVE-2010-0202, and CVE-2010-0203.
CVE-2010-0199	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0198, CVE-2010-0202, and CVE-2010-0203.
CVE-2010-0201	Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allow attackers to cause a denial of service (memory corruption) or execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0194, CVE-2010-0197, and CVE-2010-0204.
CVE-2010-0202	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0198, CVE-2010-0199, and CVE-2010-0203.
CVE-2010-0203	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0198, CVE-2010-0199, and CVE-2010-0202.
CVE-2010-0204	Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allow

	attackers to cause a denial of service (memory corruption) or execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-0194, CVE-2010-0197, and CVE-2010-0201.
CVE-2010-0209	Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2213, CVE-2010-2214, and CVE-2010-2216.
CVE-2010-0315	WebKit before r53607, as used in Google Chrome before 4.0.249.89, allows remote attackers to discover a redirect's target URL, for the session of a specific user of a web site, by placing the site's URL in the HREF attribute of a stylesheet LINK element, and then reading the document.styleSheets[0].href property value, related to an IFRAME element.
CVE-2010-0556	browser/login/login_prompt.cc in Google Chrome before 4.0.249.89 populates an authentication dialog with credentials that were stored by Password Manager for a different web site, which allows user-assisted remote HTTP servers to obtain sensitive information via a URL that requires authentication, as demonstrated by a URL in the SRC attribute of an IMG element.
CVE-2010-0643	Google Chrome before 4.0.249.89 attempts to make direct connections to web sites when all configured proxy servers are unavailable, which allows remote HTTP servers to obtain potentially sensitive information about the identity of a client user via standard HTTP logging, as demonstrated by a proxy server that was configured for the purpose of anonymity.
CVE-2010-0644	Google Chrome before 4.0.249.89, when a SOCKS 5 proxy server is configured, sends DNS queries directly, which allows remote DNS servers to obtain potentially sensitive information about the identity of a client user via request logging, as demonstrated by a proxy server that was configured for the purpose of anonymity.
CVE-2010-0645	Multiple integer overflows in factory.cc in Google V8 before r3560, as used in Google Chrome before 4.0.249.89, allow remote attackers to execute arbitrary code in the Chrome sandbox via crafted use of JavaScript arrays.
CVE-2010-0646	Multiple integer signedness errors in factory.cc in Google V8 before r3560, as used in Google Chrome before 4.0.249.89, allow remote attackers to execute arbitrary code in the Chrome sandbox via crafted use of JavaScript arrays.
CVE-2010-0647	WebKit before r53525, as used in Google Chrome before 4.0.249.89, allows remote attackers to execute arbitrary code in the Chrome sandbox via

	a malformed RUBY element, as demonstrated by a <ruby><table><rt> sequence.
CVE-2010-0649	Integer overflow in the CrossCallParamsEx::CreateFromBuffer function in sandbox/src/crosscall_server.cc in Google Chrome before 4.0.249.89 allows attackers to leverage renderer access to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via a malformed message, related to deserializing of sandbox messages.
CVE-2010-0650	WebKit, as used in Google Chrome before 4.0.249.78 and Apple Safari, allows remote attackers to bypass intended restrictions on popup windows via crafted use of a mouse click event.
CVE-2010-0651	WebKit before r52784, as used in Google Chrome before 4.0.249.78 and Apple Safari before 4.0.5, permits cross-origin loading of CSS stylesheets even when the stylesheet download has an incorrect MIME type and the stylesheet document is malformed, which allows remote attackers to obtain sensitive information via a crafted document.
CVE-2010-0655	Use-after-free vulnerability in Google Chrome before 4.0.249.78 allows user-assisted remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors involving the display of a blocked popup window during navigation to a different web site.
CVE-2010-0656	WebKit before r51295, as used in Google Chrome before 4.0.249.78, presents a directory-listing page in response to an XMLHttpRequest for a file:/// URL that corresponds to a directory, which allows attackers to obtain sensitive information or possibly have unspecified other impact via a crafted local HTML document.
CVE-2010-0658	Multiple integer overflows in Skia, as used in Google Chrome before 4.0.249.78, allow remote attackers to execute arbitrary code in the Chrome sandbox or cause a denial of service (memory corruption and application crash) via vectors involving CANVAS elements.
CVE-2010-0659	The image decoder in WebKit before r52833, as used in Google Chrome before 4.0.249.78, does not properly handle a failure of memory allocation, which allows remote attackers to execute arbitrary code in the Chrome sandbox via a malformed GIF file that specifies a large size.
CVE-2010-0660	Google Chrome before 4.0.249.78 sends an https URL in the Referer header of an http request in certain circumstances involving https to http redirection, which allows remote HTTP servers to obtain potentially sensitive information via standard HTTP logging.

CVE-2010-0661	WebCore/bindings/v8/custom/V8DOMWindowCustom.cpp in WebKit before r52401, as used in Google Chrome before 4.0.249.78, allows remote attackers to bypass the Same Origin Policy via vectors involving the window.open method.
CVE-2010-0662	The ParamTraits<SkBitmap>::Read function in common/common_param_traits.cc in Google Chrome before 4.0.249.78 does not use the correct variables in calculations designed to prevent integer overflows, which allows attackers to leverage renderer access to cause a denial of service or possibly have unspecified other impact via bitmap data, related to deserialization.
CVE-2010-0663	The ParamTraits<SkBitmap>::Read function in common/common_param_traits.cc in Google Chrome before 4.0.249.78 does not initialize the memory locations that will hold bitmap data, which might allow remote attackers to obtain potentially sensitive information from process memory by providing insufficient data, related to use of a (1) thumbnail database or (2) HTML canvas.
CVE-2010-0664	Stack consumption vulnerability in the ChildProcessSecurityPolicy::CanRequestURL function in browser/child_process_security_policy.cc in Google Chrome before 4.0.249.78 allows remote attackers to cause a denial of service (memory consumption and application crash) via a URL that specifies multiple protocols, as demonstrated by a URL that begins with many repetitions of the view-source: substring.
CVE-2010-1228	Multiple race conditions in the sandbox infrastructure in Google Chrome before 4.1.249.1036 have unspecified impact and attack vectors.
CVE-2010-1229	The sandbox infrastructure in Google Chrome before 4.1.249.1036 does not properly use pointers, which has unspecified impact and attack vectors.
CVE-2010-1230	Google Chrome before 4.1.249.1036 does not have the expected behavior for attempts to delete Web SQL Databases and clear the Strict Transport Security (STS) state, which has unspecified impact and attack vectors.
CVE-2010-1231	Google Chrome before 4.1.249.1036 processes HTTP headers before invoking the SafeBrowsing feature, which allows remote attackers to have an unspecified impact via crafted headers.
CVE-2010-1232	Google Chrome before 4.1.249.1036 allows remote attackers to cause a denial of service (memory error) or possibly have unspecified other impact via a malformed SVG document.
CVE-2010-1233	Multiple integer overflows in Google Chrome before 4.1.249.1036 allow remote attackers to have an

	unspecified impact via vectors involving WebKit JavaScript objects.
CVE-2010-1234	Unspecified vulnerability in Google Chrome before 4.1.249.1036 allows remote attackers to truncate the URL shown in the HTTP Basic Authentication dialog via unknown vectors.
CVE-2010-1235	Unspecified vulnerability in Google Chrome before 4.1.249.1036 allows remote attackers to trigger the omission of a download warning dialog via unknown vectors.
CVE-2010-1236	The protocolIs function in platform/KURLGoogle.cpp in WebCore in WebKit before r55822, as used in Google Chrome before 4.1.249.1036 and Flock Browser 3.x before 3.0.0.4112, does not properly handle whitespace at the beginning of a URL, which allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted javascript: URL, as demonstrated by a \x00javascript:alert sequence.
CVE-2010-1237	Google Chrome 4.1 BETA before 4.1.249.1036 allows remote attackers to cause a denial of service (memory error) or possibly have unspecified other impact via an empty SVG element.
CVE-2010-1240	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, do not restrict the contents of one text field in the Launch File warning dialog, which makes it easier for remote attackers to trick users into executing an arbitrary local program that was specified in a PDF document, as demonstrated by a text field that claims that the Open button will enable the user to read an encrypted message.
CVE-2010-1241	Heap-based buffer overflow in the custom heap management system in Adobe Reader and Acrobat 9.x before 9.3.2, and 8.x before 8.2.2 on Windows and Mac OS X, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted PDF document, aka FG-VD-10-005.
CVE-2010-1285	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code via unspecified manipulations involving the newclass (0x58) operator and an "invalid pointer vulnerability" that triggers memory corruption, a different vulnerability than CVE-2010-2168 and CVE-2010-2201.
CVE-2010-1293	Cross-site scripting (XSS) vulnerability in the Administrator page in Adobe ColdFusion 8.0, 8.0.1, and 9.0 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2010-1294	Unspecified vulnerability in Adobe ColdFusion 8.0, 8.0.1, and 9.0 allows local users to obtain sensitive information via unknown vectors.

CVE-2010-1295	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2202, CVE-2010-2207, CVE-2010-2209, CVE-2010-2210, CVE-2010-2211, and CVE-2010-2212.
CVE-2010-1297	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64; Adobe AIR before 2.0.2.12610; and Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted SWF content, related to authplay.dll and the ActionScript Virtual Machine 2 (AVM2) newfunction instruction, as exploited in the wild in June 2010.
CVE-2010-1487	IBM Lotus Notes 7.0, 8.0, and 8.5 stores administrative credentials in cleartext in SURunAs.exe, which allows local users to obtain sensitive information by examining this file, aka SPR JSTN837SEG.
CVE-2010-1500	Google Chrome before 4.1.249.1059 does not properly support forms, which has unknown impact and attack vectors, related to a "type confusion error."
CVE-2010-1502	Unspecified vulnerability in Google Chrome before 4.1.249.1059 allows remote attackers to access local files via vectors related to "developer tools."
CVE-2010-1503	Cross-site scripting (XSS) vulnerability in Google Chrome before 4.1.249.1059 allows remote attackers to inject arbitrary web script or HTML via vectors related to a chrome://net-internals URI.
CVE-2010-1504	Cross-site scripting (XSS) vulnerability in Google Chrome before 4.1.249.1059 allows remote attackers to inject arbitrary web script or HTML via vectors related to a chrome://downloads URI.
CVE-2010-1505	Google Chrome before 4.1.249.1059 does not prevent pages from loading with the New Tab page's privileges, which has unknown impact and attack vectors.
CVE-2010-1506	The Google V8 bindings in Google Chrome before 4.1.249.1059 allow attackers to cause a denial of service (memory corruption) via unknown vectors.
CVE-2010-1663	The Google URL Parsing Library (aka google-url or GURL) in Google Chrome before 4.1.249.1064 allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2010-1664	Google Chrome before 4.1.249.1064 does not properly handle HTML5 media, which allows remote attackers to cause a denial of service (memory corruption) and possibly have unspecified other impact via unknown vectors.

CVE-2010-1665	Google Chrome before 4.1.249.1064 does not properly handle fonts, which allows remote attackers to cause a denial of service (memory corruption) and possibly have unspecified other impact via unknown vectors.
CVE-2010-1767	Cross-site request forgery (CSRF) vulnerability in loader/DocumentThreadableLoader.cpp in WebCore in WebKit before r57041, as used in Google Chrome before 4.1.249.1059, allows remote attackers to hijack the authentication of unspecified victims via a crafted synchronous preflight XMLHttpRequest operation.
CVE-2010-1770	WebKit in Apple Safari before 5.0 on Mac OS X 10.5 through 10.6 and Windows, Apple Safari before 4.1 on Mac OS X 10.4, and Google Chrome before 5.0.375.70 does not properly handle a transformation of a text node that has the IBM1147 character set, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted HTML document containing a BR element, related to a "type checking issue."
CVE-2010-1772	Use-after-free vulnerability in page/Geolocation.cpp in WebCore in WebKit before r59859, as used in Google Chrome before 5.0.375.70, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted web site, related to failure to stop timers associated with geolocation upon deletion of a document.
CVE-2010-1773	Off-by-one error in the toAlphabetic function in rendering/RenderListMarker.cpp in WebCore in WebKit before r59950, as used in Google Chrome before 5.0.375.70, allows remote attackers to obtain sensitive information, cause a denial of service (memory corruption and application crash), or possibly execute arbitrary code via vectors related to list markers for HTML lists, aka rdar problem 8009118.
CVE-2010-1822	WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3 and Google Chrome before 6.0.472.62, does not properly perform a cast of an unspecified variable, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via an SVG element in a non-SVG document.
CVE-2010-1823	Use-after-free vulnerability in WebKit before r65958, as used in Google Chrome before 6.0.472.59, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger use of document APIs such as document.close during parsing, as demonstrated by a Cascading Style Sheets (CSS) file referencing an invalid SVG font, aka rdar problem 8442098.
CVE-2010-1824	Use-after-free vulnerability in WebKit, as used in Apple iTunes before 10.2 on Windows, Apple Safari, and

	Google Chrome before 6.0.472.59, allows remote attackers to execute arbitrary code or cause a denial of service via vectors related to SVG styles, the DOM tree, and error messages.
CVE-2010-1825	Use-after-free vulnerability in WebKit, as used in Google Chrome before 6.0.472.59, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to nested SVG elements.
CVE-2010-2105	Google Chrome before 5.0.375.55 does not properly follow the Safe Browsing specification's requirements for canonicalization of URLs, which has unspecified impact and remote attack vectors.
CVE-2010-2106	Unspecified vulnerability in Google Chrome before 5.0.375.55 might allow remote attackers to spoof the URL bar via vectors involving unload event handlers.
CVE-2010-2107	Unspecified vulnerability in Google Chrome before 5.0.375.55 allows attackers to cause a denial of service (memory error) or possibly have unspecified other impact via vectors related to the Safe Browsing functionality.
CVE-2010-2108	Unspecified vulnerability in Google Chrome before 5.0.375.55 allows remote attackers to bypass the whitelist-mode plugin blocker via unknown vectors.
CVE-2010-2109	Unspecified vulnerability in Google Chrome before 5.0.375.55 allows user-assisted remote attackers to cause a denial of service (memory error) or possibly have unspecified other impact via vectors related to the "drag + drop" functionality.
CVE-2010-2110	Google Chrome before 5.0.375.55 does not properly execute JavaScript code in the extension context, which has unspecified impact and remote attack vectors.
CVE-2010-2160	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via an invalid offset in an unspecified undocumented opcode in ActionScript Virtual Machine 2, related to getouterscope, a different vulnerability than CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2161	Array index error in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified "types of Adobe Flash code."

CVE-2010-2162	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (heap memory corruption) or possibly execute arbitrary code via vectors related to improper length calculation and the (1) STSC, (2) STSZ, and (3) STCO atoms.
CVE-2010-2163	Multiple unspecified vulnerabilities in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unknown vectors.
CVE-2010-2164	Use-after-free vulnerability in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified vectors related to an unspecified "image type within a certain function."
CVE-2010-2165	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2160, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2166	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2167	Multiple heap-based buffer overflows in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified vectors related to malformed (1) GIF or (2) JPEG data.
CVE-2010-2168	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code via a PDF file with crafted Flash content, involving the newfunction (0x44) operator and an "invalid pointer vulnerability" that triggers memory corruption, a different vulnerability than CVE-2010-1285 and CVE-2010-2201.
CVE-2010-2169	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allow

	attackers to cause a denial of service (pointer memory corruption) or possibly execute arbitrary code via unspecified vectors.
CVE-2010-2170	Integer overflow in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2181 and CVE-2010-2183.
CVE-2010-2171	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via vectors related to SWF files, decompression of embedded JPEG image data, and the DefineBits and other unspecified tags, a different vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2166, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2172	Adobe Flash Player 9 before 9.0.277.0 on unspecified UNIX platforms allows attackers to cause a denial of service via unknown vectors.
CVE-2010-2173	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified vectors, related to an "invalid pointer vulnerability" and the newclass (0x58) operator, a different vulnerability than CVE-2010-2174.
CVE-2010-2174	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified vectors, related to an "invalid pointer vulnerability" and the newfunction (0x44) operator, a different vulnerability than CVE-2010-2173.
CVE-2010-2175	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2176	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2160, CVE-2010-2165,

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

	CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2184, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2183	Integer overflow in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2170 and CVE-2010-2181.
CVE-2010-2184	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2187, and CVE-2010-2188.
CVE-2010-2185	Buffer overflow in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, might allow attackers to execute arbitrary code via unspecified vectors.
CVE-2010-2186	Unspecified vulnerability in Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2010-2187	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, and CVE-2010-2188.
CVE-2010-2188	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code by calling the ActionScript native object 2200 connect method multiple times with different arguments, a different vulnerability than CVE-2010-2160, CVE-2010-2165, CVE-2010-2166, CVE-2010-2171, CVE-2010-2175, CVE-2010-2176, CVE-2010-2177, CVE-2010-2178, CVE-2010-2180, CVE-2010-2182, CVE-2010-2184, and CVE-2010-2187.
CVE-2010-2189	Adobe Flash Player before 9.0.277.0 and 10.x before 10.1.53.64, and Adobe AIR before 2.0.2.12610, when

	used in conjunction with VMWare Tools on a VMWare platform, allows attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via unspecified vectors.
CVE-2010-2201	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code via a PDF file with crafted Flash content involving the (1) pushstring (0x2C) operator, (2) debugfile (0xF1) operator, and an "invalid pointer vulnerability" that triggers memory corruption, a different vulnerability than CVE-2010-1285 and CVE-2010-2168.
CVE-2010-2202	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-1295, CVE-2010-2207, CVE-2010-2209, CVE-2010-2210, CVE-2010-2211, and CVE-2010-2212.
CVE-2010-2203	Adobe Reader and Acrobat 9.x before 9.3.3 on UNIX allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2010-2204	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors.
CVE-2010-2205	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, access uninitialized memory, which allows attackers to execute arbitrary code via unspecified vectors.
CVE-2010-2206	Array index error in AcroForm.api in Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allows remote attackers to execute arbitrary code via a crafted GIF image in a PDF file, which bypasses a size check and triggers a heap-based buffer overflow.
CVE-2010-2207	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-1295, CVE-2010-2202, CVE-2010-2209, CVE-2010-2210, CVE-2010-2211, and CVE-2010-2212.
CVE-2010-2208	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, dereference a heap object after this object's deletion, which allows attackers to execute arbitrary code via unspecified vectors.

CVE-2010-2209	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-1295, CVE-2010-2202, CVE-2010-2207, CVE-2010-2210, CVE-2010-2211, and CVE-2010-2212.
CVE-2010-2210	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-1295, CVE-2010-2202, CVE-2010-2207, CVE-2010-2209, CVE-2010-2211, and CVE-2010-2212.
CVE-2010-2211	Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-1295, CVE-2010-2202, CVE-2010-2207, CVE-2010-2209, CVE-2010-2210, and CVE-2010-2212.
CVE-2010-2212	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.3.3, and 8.x before 8.2.3 on Windows and Mac OS X, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via a PDF file containing Flash content with a crafted #1023 (3FFh) tag, a different vulnerability than CVE-2010-1295, CVE-2010-2202, CVE-2010-2207, CVE-2010-2209, CVE-2010-2210, and CVE-2010-2211.
CVE-2010-2213	Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-0209, CVE-2010-2214, and CVE-2010-2216.
CVE-2010-2214	Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-0209, CVE-2010-2213, and CVE-2010-2216.
CVE-2010-2215	Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to trick a user into (1) selecting a link or (2) completing a dialog, related to a "click-jacking" issue.
CVE-2010-2216	Adobe Flash Player before 9.0.280 and 10.x before 10.1.82.76, and Adobe AIR before 2.0.3, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified

	vectors, a different vulnerability than CVE-2010-0209, CVE-2010-2213, and CVE-2010-2214.
CVE-2010-2295	page/EventHandler.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 does not properly handle a change of the focused frame during the dispatching of keydown, which allows user-assisted remote attackers to redirect keystrokes via a crafted HTML document, aka rdar problem 7018610. NOTE: this might overlap CVE-2010-1422.
CVE-2010-2296	The implementation of unspecified DOM methods in Google Chrome before 5.0.375.70 allows remote attackers to bypass the Same Origin Policy via unknown vectors.
CVE-2010-2297	rendering/FixedTableLayout.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via an HTML document that has a large colspan attribute within a table.
CVE-2010-2298	browser/renderer_host/database_dispatcher_host.cc in Google Chrome before 5.0.375.70 on Linux does not properly handle ViewHostMsg_DatabaseOpenFile messages in chroot-based sandboxing, which allows remote attackers to bypass intended sandbox restrictions via vectors involving fchdir and chdir calls.
CVE-2010-2299	The Clipboard::DispatchObject function in app/clipboard/clipboard.cc in Google Chrome before 5.0.375.70 does not properly handle CBF_SMBITMAP objects in a ViewHostMsg_ClipboardWriteObjectsAsync message, which might allow remote attackers to execute arbitrary code via vectors involving crafted data from the renderer process, related to a "Type Confusion" issue.
CVE-2010-2300	Use-after-free vulnerability in the Element::normalizeAttributes function in dom/Element.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via vectors related to handlers for DOM mutation events, aka rdar problem 7948784. NOTE: this might overlap CVE-2010-1759.
CVE-2010-2301	Cross-site scripting (XSS) vulnerability in editing/markup.cpp in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to inject arbitrary web script or HTML via vectors related to the node.innerHTML property of a TEXTAREA element. NOTE: this might overlap CVE-2010-1762.
CVE-2010-2302	Use-after-free vulnerability in WebCore in WebKit in Google Chrome before 5.0.375.70 allows remote attackers to cause a denial of service (memory

	corruption) or possibly execute arbitrary code via vectors involving remote fonts in conjunction with shadow DOM trees, aka rdar problem 8007953. NOTE: this might overlap CVE-2010-1771.
CVE-2010-2455	Opera does not properly manage the address bar between the request to open a URL and the retrieval of the new document's content, which might allow remote attackers to conduct spoofing attacks via a crafted HTML document, a related issue to CVE-2010-1206.
CVE-2010-2645	Unspecified vulnerability in Google Chrome before 5.0.375.99, when WebGL is used, allows remote attackers to cause a denial of service (out-of-bounds read) via unknown vectors.
CVE-2010-2646	Google Chrome before 5.0.375.99 does not properly isolate sandboxed IFRAME elements, which has unspecified impact and remote attack vectors.
CVE-2010-2647	Google Chrome before 5.0.375.99 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via an invalid SVG document.
CVE-2010-2648	The implementation of the Unicode Bidirectional Algorithm (aka Bidi algorithm or UBA) in Google Chrome before 5.0.375.99 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-2649	Unspecified vulnerability in Google Chrome before 5.0.375.99 allows remote attackers to cause a denial of service (application crash) via an invalid image.
CVE-2010-2650	Unspecified vulnerability in Google Chrome before 5.0.375.99 has unknown impact and attack vectors, related to an "annoyance with print dialogs."
CVE-2010-2651	The Cascading Style Sheets (CSS) implementation in Google Chrome before 5.0.375.99 does not properly perform style rendering, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-2652	Google Chrome before 5.0.375.99 does not properly implement modal dialogs, which allows attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2010-2861	Multiple directory traversal vulnerabilities in the administrator console in Adobe ColdFusion 9.0.1 and earlier allow remote attackers to read arbitrary files via the locale parameter to (1) CFIDE/administrator/settings/mappings.cfm, (2) logging/settings.cfm, (3) datasources/index.cfm, (4) j2eepackaging/

	editarchive.cfm, and (5) enter.cfm in CFIDE/administrator/.
CVE-2010-2862	Integer overflow in CoolType.dll in Adobe Reader 8.2.3 and 9.3.3, and Acrobat 9.3.3, allows remote attackers to execute arbitrary code via a TrueType font with a large maxCompositePoints value in a Maximum Profile (maxp) table.
CVE-2010-2883	Stack-based buffer overflow in CoolType.dll in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a PDF document with a long field in a Smart INdependent Glyphlets (SING) table in a TTF font, as exploited in the wild in September 2010. NOTE: some of these details are obtained from third party information.
CVE-2010-2884	Adobe Flash Player 10.1.82.76 and earlier on Windows, Mac OS X, Linux, and Solaris and 10.1.92.10 on Android; authplay.dll in Adobe Reader and Acrobat 9.x before 9.4; and authplay.dll in Adobe Reader and Acrobat 8.x before 8.2.5 on Windows and Mac OS X allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as exploited in the wild in September 2010.
CVE-2010-2887	Multiple unspecified vulnerabilities in Adobe Reader and Acrobat 9.x before 9.4 on Linux allow attackers to gain privileges via unknown vectors.
CVE-2010-2889	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to execute arbitrary code via a crafted font, a different vulnerability than CVE-2010-3626.
CVE-2010-2890	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-3619, CVE-2010-3621, CVE-2010-3622, CVE-2010-3628, CVE-2010-3632, and CVE-2010-3658.
CVE-2010-2897	Google Chrome before 5.0.375.125 does not properly mitigate an unspecified flaw in the Windows kernel, which has unknown impact and attack vectors.
CVE-2010-2898	Google Chrome before 5.0.375.125 does not properly mitigate an unspecified flaw in the GNU C Library, which has unknown impact and attack vectors.
CVE-2010-2899	Unspecified vulnerability in the layout implementation in Google Chrome before 5.0.375.125 allows remote attackers to obtain sensitive information from process memory via unknown vectors.

CVE-2010-2900	Google Chrome before 5.0.375.125 does not properly handle a large canvas, which has unspecified impact and remote attack vectors.
CVE-2010-2901	The rendering implementation in Google Chrome before 5.0.375.125 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-2902	The SVG implementation in Google Chrome before 5.0.375.125 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-2903	Google Chrome before 5.0.375.125 performs unexpected truncation and improper eliding of hostnames, which has unspecified impact and remote attack vectors.
CVE-2010-3112	Google Chrome before 5.0.375.127 does not properly implement file dialogs, which allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3113	Google Chrome before 5.0.375.127, and webkitgtk before 1.2.5, does not properly handle SVG documents, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors related to state changes when using DeleteButtonController.
CVE-2010-3114	The text-editing implementation in Google Chrome before 5.0.375.127, and webkitgtk before 1.2.6, does not check a node type before performing a cast, which has unspecified impact and attack vectors related to (1) DeleteSelectionCommand.cpp, (2) InsertLineBreakCommand.cpp, or (3) InsertParagraphSeparatorCommand.cpp in WebCore/editing/.
CVE-2010-3115	Google Chrome before 5.0.375.127, and webkitgtk before 1.2.6, does not properly implement the history feature, which might allow remote attackers to spoof the address bar via unspecified vectors.
CVE-2010-3116	Multiple use-after-free vulnerabilities in WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3, Google Chrome before 5.0.375.127, and webkitgtk before 1.2.6, allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors related to improper handling of MIME types by plug-ins.
CVE-2010-3117	Google Chrome before 5.0.375.127 does not properly implement the notifications feature, which allows remote attackers to cause a denial of service (application crash) and possibly have unspecified other impact via unknown vectors.

CVE-2010-3118	The autosuggest feature in the Omnibox implementation in Google Chrome before 5.0.375.127 does not anticipate entry of passwords, which might allow remote attackers to obtain sensitive information by reading the network traffic generated by this feature.
CVE-2010-3119	Google Chrome before 5.0.375.127 and webkitgtk before 1.2.6 do not properly support the Ruby language, which allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3120	Google Chrome before 5.0.375.127 does not properly implement the Geolocation feature, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3246	Google Chrome before 6.0.472.53 does not properly handle the _blank value for the target attribute of unspecified elements, which allows remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2010-3247	Google Chrome before 6.0.472.53 does not properly restrict the characters in URLs, which allows remote attackers to spoof the appearance of the URL bar via homographic sequences.
CVE-2010-3248	Google Chrome before 6.0.472.53 does not properly restrict copying to the clipboard, which has unspecified impact and attack vectors.
CVE-2010-3249	Google Chrome before 6.0.472.53 does not properly implement SVG filters, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, related to a "stale pointer" issue.
CVE-2010-3250	Unspecified vulnerability in Google Chrome before 6.0.472.53 allows remote attackers to enumerate the set of installed extensions via unknown vectors.
CVE-2010-3251	The WebSockets implementation in Google Chrome before 6.0.472.53 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via unspecified vectors.
CVE-2010-3252	Use-after-free vulnerability in the Notifications presenter in Google Chrome before 6.0.472.53 allows attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2010-3253	The implementation of notification permissions in Google Chrome before 6.0.472.53 allows attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3254	The WebSockets implementation in Google Chrome before 6.0.472.53 does not properly handle integer

	values, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2010-3255	Google Chrome before 6.0.472.53 and webkitgtk before 1.2.6 do not properly handle counter nodes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3256	Google Chrome before 6.0.472.53 does not properly limit the number of stored autocomplete entries, which has unspecified impact and attack vectors.
CVE-2010-3257	Use-after-free vulnerability in WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3, Google Chrome before 6.0.472.53, and webkitgtk before 1.2.6, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via vectors involving element focus.
CVE-2010-3258	The sandbox implementation in Google Chrome before 6.0.472.53 does not properly deserialize parameters, which has unspecified impact and remote attack vectors.
CVE-2010-3259	WebKit, as used in Apple Safari before 4.1.3 and 5.0.x before 5.0.3, Google Chrome before 6.0.472.53, and webkitgtk before 1.2.6, does not properly restrict read access to images derived from CANVAS elements, which allows remote attackers to bypass the Same Origin Policy and obtain potentially sensitive image data via a crafted web site.
CVE-2010-3411	Google Chrome before 6.0.472.59 on Linux does not properly handle cursors, which might allow attackers to cause a denial of service (assertion failure) via unspecified vectors.
CVE-2010-3412	Race condition in the console implementation in Google Chrome before 6.0.472.59 has unspecified impact and attack vectors.
CVE-2010-3413	Unspecified vulnerability in the pop-up blocking functionality in Google Chrome before 6.0.472.59 allows remote attackers to cause a denial of service (application crash) via unknown vectors.
CVE-2010-3415	Google Chrome before 6.0.472.59 does not properly implement Geolocation, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2010-3416	Google Chrome before 6.0.472.59 on Linux does not properly implement the Khmer locale, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.

CVE-2010-3417	Google Chrome before 6.0.472.59 does not prompt the user before granting access to the extension history, which allows attackers to obtain potentially sensitive information via unspecified vectors.
CVE-2010-3474	IBM DB2 9.7 before FP3 does not perform the expected drops or invalidations of dependent functions upon a loss of privileges by the functions' owners, which allows remote authenticated users to bypass intended access restrictions via calls to these functions, a different vulnerability than CVE-2009-3471.
CVE-2010-3475	IBM DB2 9.7 before FP3 does not properly enforce privilege requirements for execution of entries in the dynamic SQL cache, which allows remote authenticated users to bypass intended access restrictions by leveraging the cache to execute an UPDATE statement contained in a compiled compound SQL statement.
CVE-2010-3619	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2890, CVE-2010-3621, CVE-2010-3622, CVE-2010-3628, CVE-2010-3632, and CVE-2010-3658.
CVE-2010-3620	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to execute arbitrary code via a crafted image, a different vulnerability than CVE-2010-3629.
CVE-2010-3621	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2890, CVE-2010-3619, CVE-2010-3622, CVE-2010-3628, CVE-2010-3632, and CVE-2010-3658.
CVE-2010-3622	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2890, CVE-2010-3619, CVE-2010-3621, CVE-2010-3628, CVE-2010-3632, and CVE-2010-3658.
CVE-2010-3625	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code via unspecified vectors, related to a "prefix protocol handler vulnerability."
CVE-2010-3626	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to execute arbitrary

	code via a crafted font, a different vulnerability than CVE-2010-2889.
CVE-2010-3627	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to execute arbitrary code via unknown vectors.
CVE-2010-3628	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2890, CVE-2010-3619, CVE-2010-3621, CVE-2010-3622, CVE-2010-3632, and CVE-2010-3658.
CVE-2010-3629	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to execute arbitrary code via a crafted image, a different vulnerability than CVE-2010-3620.
CVE-2010-3630	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors.
CVE-2010-3632	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2890, CVE-2010-3619, CVE-2010-3621, CVE-2010-3622, CVE-2010-3628, and CVE-2010-3658.
CVE-2010-3636	Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, does not properly handle unspecified encodings during the parsing of a cross-domain policy file, which allows remote web servers to bypass intended access restrictions via unknown vectors.
CVE-2010-3639	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors.
CVE-2010-3640	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646,

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

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

	CVE-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, and CVE-2010-3652.
CVE-2010-3652	Unspecified vulnerability in Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris, and 10.1.95.1 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, a different vulnerability than CVE-2010-3640, CVE-2010-3641, CVE-2010-3642, CVE-2010-3643, CVE-2010-3644, CVE-2010-3645, CVE-2010-3646, CVE-2010-3647, CVE-2010-3648, CVE-2010-3649, and CVE-2010-3650.
CVE-2010-3654	Adobe Flash Player before 9.0.289.0 and 10.x before 10.1.102.64 on Windows, Mac OS X, Linux, and Solaris and 10.1.95.1 on Android, and authplay.dll (aka AuthPlayLib.bundle or libauthplay.so.0.0.0) in Adobe Reader and Acrobat 9.x through 9.4, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via crafted SWF content, as exploited in the wild in October 2010.
CVE-2010-3656	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to cause a denial of service via unknown vectors, a different vulnerability than CVE-2010-3657.
CVE-2010-3657	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allows attackers to cause a denial of service via unknown vectors, a different vulnerability than CVE-2010-3656.
CVE-2010-3658	Adobe Reader and Acrobat 9.x before 9.4, and 8.x before 8.2.5 on Windows and Mac OS X, allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2010-2890, CVE-2010-3619, CVE-2010-3621, CVE-2010-3622, CVE-2010-3628, and CVE-2010-3632.
CVE-2010-3729	The SPDY protocol implementation in Google Chrome before 6.0.472.62 does not properly manage buffers, which might allow remote attackers to execute arbitrary code via unspecified vectors.
CVE-2010-3730	Google Chrome before 6.0.472.62 does not properly use information about the origin of a document to manage properties, which allows remote attackers to have an unspecified impact via a crafted web site, related to a "property pollution" issue.
CVE-2010-3864	Multiple race conditions in ssl/t1_lib.c in OpenSSL 0.9.8f through 0.9.8o, 1.0.0, and 1.0.0a, when multi-threading and internal caching are enabled on a

	TLS server, might allow remote attackers to execute arbitrary code via client data that triggers a heap-based buffer overflow, related to (1) the TLS server name extension and (2) elliptic curve cryptography.
CVE-2010-4008	libxml2 before 2.7.8, as used in Google Chrome before 7.0.517.44, Apple Safari 5.0.2 and earlier, and other products, reads from invalid memory locations during processing of malformed XPath expressions, which allows context-dependent attackers to cause a denial of service (application crash) via a crafted XML document.
CVE-2010-4033	Google Chrome before 7.0.517.41 does not properly implement the autofill and autocomplete functionality, which allows remote attackers to conduct "profile spamming" attacks via unspecified vectors.
CVE-2010-4034	Google Chrome before 7.0.517.41 does not properly handle forms, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.
CVE-2010-4035	Google Chrome before 7.0.517.41 does not properly perform autofill operations for forms, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.
CVE-2010-4036	Google Chrome before 7.0.517.41 does not properly handle the unloading of a page, which allows remote attackers to spoof URLs via unspecified vectors.
CVE-2010-4037	Unspecified vulnerability in Google Chrome before 7.0.517.41 allows remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2010-4038	The Web Sockets implementation in Google Chrome before 7.0.517.41 does not properly handle a shutdown action, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2010-4039	Google Chrome before 7.0.517.41 on Linux does not properly set the PATH environment variable, which has unspecified impact and attack vectors.
CVE-2010-4040	Google Chrome before 7.0.517.41 does not properly handle animated GIF images, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted image.
CVE-2010-4041	The sandbox implementation in Google Chrome before 7.0.517.41 on Linux does not properly constrain worker processes, which might allow remote attackers to bypass intended access restrictions via unspecified vectors.
CVE-2010-4042	Google Chrome before 7.0.517.41 does not properly handle element maps, which allows remote attackers to

	cause a denial of service or possibly have unspecified other impact via vectors related to "stale elements."
CVE-2010-4091	The EScript.api plugin in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.1, and 8.x before 8.2.6 on Windows and Mac OS X allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a crafted PDF document that triggers memory corruption, involving the printSeps function. NOTE: some of these details are obtained from third party information.
CVE-2010-4197	Use-after-free vulnerability in WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving text editing.
CVE-2010-4198	WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, does not properly handle large text areas, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted HTML document.
CVE-2010-4199	Google Chrome before 7.0.517.44 does not properly perform a cast of an unspecified variable during processing of an SVG use element, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted SVG document.
CVE-2010-4201	Use-after-free vulnerability in Google Chrome before 7.0.517.44 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving text control selections.
CVE-2010-4202	Multiple integer overflows in Google Chrome before 7.0.517.44 on Linux allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted font.
CVE-2010-4203	WebM libvpx (aka the VP8 Codec SDK) before 0.9.5, as used in Google Chrome before 7.0.517.44, allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via invalid frames.
CVE-2010-4204	WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, accesses a frame object after this object has been destroyed, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2010-4205	Google Chrome before 7.0.517.44 does not properly handle the data types of event objects, which allows remote attackers to cause a denial of service or

	possibly have unspecified other impact via unknown vectors.
CVE-2010-4206	Array index error in the FEBlend::apply function in WebCore/platform/graphics/filters/FEBlend.cpp in WebKit, as used in Google Chrome before 7.0.517.44, webkitgtk before 1.2.6, and other products, allows remote attackers to cause a denial of service and possibly execute arbitrary code via a crafted SVG document, related to effects in the application of filters.
CVE-2010-4482	Unspecified vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2010-4483	Google Chrome before 8.0.552.215 does not properly restrict read access to videos derived from CANVAS elements, which allows remote attackers to bypass the Same Origin Policy and obtain potentially sensitive video data via a crafted web site.
CVE-2010-4484	Google Chrome before 8.0.552.215 does not properly handle HTML5 databases, which allows attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2010-4485	Google Chrome before 8.0.552.215 does not properly restrict the generation of file dialogs, which allows remote attackers to cause a denial of service (reduced usability and possible application crash) via a crafted web site.
CVE-2010-4486	Use-after-free vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to history handling.
CVE-2010-4487	Incomplete blacklist vulnerability in Google Chrome before 8.0.552.215 on Linux and Mac OS X allows remote attackers to have an unspecified impact via a "dangerous file."
CVE-2010-4488	Google Chrome before 8.0.552.215 does not properly handle HTTP proxy authentication, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2010-4489	libvpx, as used in Google Chrome before 8.0.552.215 and possibly other products, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WebM video. NOTE: this vulnerability exists because of a regression.
CVE-2010-4490	Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via malformed video content that triggers an indexing error.
CVE-2010-4491	Google Chrome before 8.0.552.215 does not properly restrict privileged extensions, which allows remote

	attackers to cause a denial of service (memory corruption) via a crafted extension.
CVE-2010-4492	Use-after-free vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG animations.
CVE-2010-4493	Use-after-free vulnerability in Google Chrome before 8.0.552.215 allows remote attackers to cause a denial of service via vectors related to the handling of mouse dragging events.
CVE-2010-4494	Double free vulnerability in libxml2 2.7.8 and other versions, as used in Google Chrome before 8.0.552.215 and other products, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XPath handling.
CVE-2010-4574	The Pickle::Pickle function in base/pickle.cc in Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 on 64-bit Linux platforms does not properly perform pointer arithmetic, which allows remote attackers to bypass message deserialization validation, and cause a denial of service or possibly have unspecified other impact, via invalid pickle data.
CVE-2010-4575	The ThemeInstalledInfoBarDelegate::Observe function in browser/extensions/theme_installed_infobar_delegate.cc in Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 does not properly handle incorrect tab interaction by an extension, which allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted extension.
CVE-2010-4576	browser/worker_host/message_port_dispatcher.cc in Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 does not properly handle certain postMessage calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted JavaScript code that creates a web worker.
CVE-2010-4577	The CSSParser::parseFontFaceSrc function in WebCore/css/CSSParser.cpp in WebKit, as used in Google Chrome before 8.0.552.224, Chrome OS before 8.0.552.343, webkitgtk before 1.2.6, and other products does not properly parse Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted local font, related to "Type Confusion."
CVE-2010-4578	Google Chrome before 8.0.552.224 and Chrome OS before 8.0.552.343 do not properly perform cursor handling, which allows remote attackers to cause a

	denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale pointers."
CVE-2010-4579	Opera before 11.00 does not properly constrain dialogs to appear on top of rendered documents, which makes it easier for remote attackers to trick users into interacting with a crafted web site that spoofs the (1) security information dialog or (2) download dialog.
CVE-2010-4580	Opera before 11.00 does not clear WAP WML form fields after manual navigation to a new web site, which allows remote attackers to obtain sensitive information via an input field that has the same name as an input field on a previously visited web site.
CVE-2010-4581	Unspecified vulnerability in Opera before 11.00 has unknown impact and attack vectors, related to "a high severity issue."
CVE-2010-4582	Opera before 11.00 does not properly handle security policies during updates to extensions, which might allow remote attackers to bypass intended access restrictions via unspecified vectors.
CVE-2010-4583	Opera before 11.00, when Opera Turbo is enabled, does not display a page's security indication, which makes it easier for remote attackers to spoof trusted content via a crafted web site.
CVE-2010-4584	Opera before 11.00, when Opera Turbo is used, does not properly present information about problematic X.509 certificates on https web sites, which might make it easier for remote attackers to spoof trusted content via a crafted web site.
CVE-2010-4585	Unspecified vulnerability in the auto-update functionality in Opera before 11.00 allows remote attackers to cause a denial of service (application crash) by triggering an Opera Unite update.
CVE-2010-4586	The default configuration of Opera before 11.00 enables WebSockets functionality, which has unspecified impact and remote attack vectors, possibly a related issue to CVE-2010-4508.
CVE-2010-4604	Stack-based buffer overflow in the GeneratePassword function in dsmtca (aka the Trusted Communications Agent or TCA) in the backup-archive client in IBM Tivoli Storage Manager (TSM) 5.3.x before 5.3.6.10, 5.4.x before 5.4.3.4, 5.5.x before 5.5.2.10, and 6.1.x before 6.1.3.1 on Unix and Linux allows local users to gain privileges by specifying a long LANG environment variable, and then sending a request over a pipe.
CVE-2010-4605	Unspecified vulnerability in the backup-archive client in IBM Tivoli Storage Manager (TSM) 5.3.x before 5.3.6.10, 5.4.x before 5.4.3.4, 5.5.x before 5.5.3, 6.1.x before 6.1.4, and 6.2.x before 6.2.2 on Unix and

	Linux allows local users to overwrite arbitrary files via unknown vectors.
CVE-2010-4606	Unspecified vulnerability in the Space Management client in the Hierarchical Storage Management (HSM) component in IBM Tivoli Storage Manager (TSM) 5.4.x before 5.4.3.4, 5.5.x before 5.5.3, 6.1.x before 6.1.4, and 6.2.x before 6.2.2 on Unix and Linux allows remote attackers to execute arbitrary commands via unknown vectors, related to a "script execution vulnerability."
CVE-2010-4785	The do_extendedOp function in ibmslapd in IBM Tivoli Directory Server (TDS) 6.0 before 6.0.0.62 (aka 6.0.0.8-TIV-ITDS-IF0004) on Linux, Solaris, and Windows allows remote authenticated users to cause a denial of service (ABEND) via a malformed LDAP extended operation that triggers certain comparisons involving the NULL operation OID.
CVE-2010-4786	IBM Tivoli Directory Server (TDS) 6.0 before 6.0.0.63 (aka 6.0.0.8-TIV-ITDS-IF0005) allows remote authenticated users to cause a denial of service (daemon crash or hang) via a paged search, as demonstrated by a certain idsldapsearch command, related to an improper ibm-slapdIdleTimeOut configuration setting.
CVE-2010-4787	IBM Tivoli Directory Server (TDS) 6.0 before 6.0.0.63 (aka 6.0.0.8-TIV-ITDS-IF0005) allows remote authenticated users to cause a denial of service (daemon hang) via a paged search that triggers improper mutex processing.
CVE-2010-4788	IBM Tivoli Directory Server (TDS) 6.0 before 6.0.0.62 (aka 6.0.0.8-TIV-ITDS-IF0004) does not perform certain locking of linked-list access, which allows remote authenticated users to cause a denial of service (daemon crash) via a paged search.
CVE-2010-4789	Use-after-free vulnerability in the proxy-server implementation in IBM Tivoli Directory Server (TDS) 6.0 before 6.0.0.65 (aka 6.0.0.8-TIV-ITDS-IF0007) and 6.3 before 6.3.0.1 (aka 6.3.0.0-TIV-ITDS-IF0001) allows remote authenticated users to cause a denial of service (daemon crash) via a paged search that is interrupted by an LDAP Unbind operation.
CVE-2011-0277	Cross-site request forgery (CSRF) vulnerability in HP Power Manager (HPPM) 4.3.2 and earlier allows remote attackers to hijack the authentication of administrators for requests that create new administrative accounts.
CVE-2011-0470	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle extensions notification, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.

CVE-2011-0471	The node-iteration implementation in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 does not properly handle pointers, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-0472	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle the printing of PDF documents, which allows user-assisted remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a multi-page document.
CVE-2011-0473	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle Cascading Style Sheets (CSS) token sequences in conjunction with CANVAS elements, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-0474	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle Cascading Style Sheets (CSS) token sequences in conjunction with cursors, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-0475	Use-after-free vulnerability in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a PDF document.
CVE-2011-0476	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 allow remote attackers to cause a denial of service (stack memory corruption) or possibly have unspecified other impact via a PDF document that triggers an out-of-memory error.
CVE-2011-0477	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle a mismatch in video frame sizes, which allows remote attackers to cause a denial of service (incorrect memory access) or possibly have unspecified other impact via unknown vectors.
CVE-2011-0478	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle SVG use elements, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-0479	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly interact with extensions, which allows remote attackers to cause a

	denial of service via a crafted extension that triggers an uninitialized pointer.
CVE-2011-0480	Multiple buffer overflows in vorbis_dec.c in the Vorbis decoder in FFmpeg, as used in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344, allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via a crafted WebM file, related to buffers for (1) the channel floor and (2) the channel residue.
CVE-2011-0481	Buffer overflow in Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to PDF shading.
CVE-2011-0482	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly perform a cast of an unspecified variable during handling of anchors, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted HTML document.
CVE-2011-0483	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly perform a cast of an unspecified variable during handling of video, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-0484	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly perform DOM node removal, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale rendering node."
CVE-2011-0485	Google Chrome before 8.0.552.237 and Chrome OS before 8.0.552.344 do not properly handle speech data, which allows remote attackers to execute arbitrary code via unspecified vectors that lead to a "stale pointer."
CVE-2011-0558	Integer overflow in Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code via a large array length value in the ActionScript method of the Function class.
CVE-2011-0559	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted parameters to an unspecified ActionScript method that cause a parameter to be used as an object pointer, a different vulnerability than CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.

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

	directory, a different vulnerability than CVE-2011-0562 and CVE-2011-0588.
CVE-2011-0571	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.
CVE-2011-0572	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.
CVE-2011-0573	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0574, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.
CVE-2011-0574	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0578, CVE-2011-0607, and CVE-2011-0608.
CVE-2011-0575	Untrusted search path vulnerability in Adobe Flash Player before 10.2.152.26 allows local users to gain privileges via a Trojan horse DLL in the current working directory.
CVE-2011-0577	Unspecified vulnerability in Adobe Flash Player before 10.2.152.26 allows remote attackers to execute arbitrary code via a crafted font.
CVE-2011-0578	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors related to a constructor for an unspecified ActionScript3 object and improper type checking, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0607, and CVE-2011-0608.
CVE-2011-0579	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to obtain sensitive information via unspecified vectors.

CVE-2011-0585	Unspecified vulnerability in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allows attackers to cause a denial of service or possibly execute arbitrary code via unknown vectors, a different vulnerability than CVE-2011-0565.
CVE-2011-0586	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X do not properly validate unspecified input data, which allows attackers to execute arbitrary code via unknown vectors.
CVE-2011-0587	Cross-site scripting (XSS) vulnerability in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2011-0604.
CVE-2011-0588	Untrusted search path vulnerability in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows allows local users to gain privileges via a Trojan horse DLL in the current working directory, a different vulnerability than CVE-2011-0562 and CVE-2011-0570.
CVE-2011-0589	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0563 and CVE-2011-0606.
CVE-2011-0590	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a 3D file, a different vulnerability than CVE-2011-0591, CVE-2011-0592, CVE-2011-0593, CVE-2011-0595, and CVE-2011-0600.
CVE-2011-0591	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a crafted Universal 3D (U3D) file that triggers a buffer overflow during decompression, related to Texture and rgba, a different vulnerability than CVE-2011-0590, CVE-2011-0592, CVE-2011-0593, CVE-2011-0595, and CVE-2011-0600.
CVE-2011-0592	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a crafted Universal 3D (U3D) file that triggers a buffer overflow during decompression, related to "Texture bmp," a different vulnerability than

	CVE-2011-0590, CVE-2011-0591, CVE-2011-0593, CVE-2011-0595, and CVE-2011-0600.
CVE-2011-0593	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a crafted Universal 3D (U3D) file that triggers a buffer overflow during decompression, a different vulnerability than CVE-2011-0590, CVE-2011-0591, CVE-2011-0592, CVE-2011-0595, and CVE-2011-0600.
CVE-2011-0594	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a font.
CVE-2011-0595	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a crafted Universal 3D (U3D) file that triggers a buffer overflow during decompression, a different vulnerability than CVE-2011-0590, CVE-2011-0591, CVE-2011-0592, CVE-2011-0593, and CVE-2011-0600.
CVE-2011-0596	The Bitmap parsing component in 2d.dll in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via an image with crafted (1) height and (2) width values for an RLE_8 compressed bitmap, which triggers a heap-based buffer overflow, a different vulnerability than CVE-2011-0598, CVE-2011-0599, and CVE-2011-0602.
CVE-2011-0598	Integer overflow in ACE.dll in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allows remote attackers to execute arbitrary code via crafted ICC data, a different vulnerability than CVE-2011-0596, CVE-2011-0599, and CVE-2011-0602.
CVE-2011-0599	The Bitmap parsing component in rt3d.dll in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a crafted image that causes an invalid pointer calculation related to 4/8-bit RLE compression, a different vulnerability than CVE-2011-0596, CVE-2011-0598, and CVE-2011-0602.
CVE-2011-0600	The U3D component in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via a 3D file with an invalid Parent Node count that triggers an incorrect size calculation and memory corruption,

	a different vulnerability than CVE-2011-0590, CVE-2011-0591, CVE-2011-0592, CVE-2011-0593, and CVE-2011-0595.
CVE-2011-0602	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code via crafted JP2K record types in a JPEG2000 image in a PDF file, which causes heap corruption, a different vulnerability than CVE-2011-0596, CVE-2011-0598, and CVE-2011-0599.
CVE-2011-0603	Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted image, a different vulnerability than CVE-2011-0566 and CVE-2011-0567.
CVE-2011-0604	Cross-site scripting (XSS) vulnerability in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allows remote attackers to inject arbitrary web script or HTML via unspecified vectors, a different vulnerability than CVE-2011-0587.
CVE-2011-0606	Stack-based buffer overflow in rt3d.dll in Adobe Reader and Acrobat 10.x before 10.0.1, 9.x before 9.4.2, and 8.x before 8.2.6 on Windows and Mac OS X allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors related to a crafted length value, a different vulnerability than CVE-2011-0563 and CVE-2011-0589.
CVE-2011-0607	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, and CVE-2011-0608.
CVE-2011-0608	Adobe Flash Player before 10.2.152.26 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0559, CVE-2011-0560, CVE-2011-0561, CVE-2011-0571, CVE-2011-0572, CVE-2011-0573, CVE-2011-0574, CVE-2011-0578, and CVE-2011-0607.
CVE-2011-0609	Unspecified vulnerability in Adobe Flash Player 10.2.154.13 and earlier on Windows, Mac OS X, Linux, and Solaris; 10.1.106.16 and earlier on Android; Adobe AIR 2.5.1 and earlier; and Authplay.dll (aka AuthPlayLib.bundle) in Adobe Reader and Acrobat 9.x through 9.4.2 and 10.x through 10.0.1 on Windows and Mac OS X, allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via

	crafted Flash content, as demonstrated by a .swf file embedded in an Excel spreadsheet, and as exploited in the wild in March 2011.
CVE-2011-0611	Adobe Flash Player before 10.2.154.27 on Windows, Mac OS X, Linux, and Solaris and 10.2.156.12 and earlier on Android; Adobe AIR before 2.6.19140; and Authplay.dll (aka AuthPlayLib.bundle) in Adobe Reader 9.x before 9.4.4 and 10.x through 10.0.1 on Windows, Adobe Reader 9.x before 9.4.4 and 10.x before 10.0.3 on Mac OS X, and Adobe Acrobat 9.x before 9.4.4 and 10.x before 10.0.3 on Windows and Mac OS X allow remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted Flash content; as demonstrated by a Microsoft Office document with an embedded .swf file that has a size inconsistency in a "group of included constants," object type confusion, ActionScript that adds custom functions to prototypes, and Date objects; and as exploited in the wild in April 2011.
CVE-2011-0612	Adobe Flash Media Server (FMS) before 3.5.6, and 4.x before 4.0.2, allows remote attackers to cause a denial of service (XML data corruption) via unspecified vectors.
CVE-2011-0618	Integer overflow in Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-0619	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0620, CVE-2011-0621, and CVE-2011-0622.
CVE-2011-0620	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0619, CVE-2011-0621, and CVE-2011-0622.
CVE-2011-0621	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0619, CVE-2011-0620, and CVE-2011-0622.
CVE-2011-0622	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code

	or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-0619, CVE-2011-0620, and CVE-2011-0621.
CVE-2011-0623	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different vulnerability than CVE-2011-0624, CVE-2011-0625, and CVE-2011-0626.
CVE-2011-0624	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different vulnerability than CVE-2011-0623, CVE-2011-0625, and CVE-2011-0626.
CVE-2011-0625	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different vulnerability than CVE-2011-0623, CVE-2011-0624, and CVE-2011-0626.
CVE-2011-0626	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows attackers to execute arbitrary code via unspecified vectors, related to a "bounds checking" issue, a different vulnerability than CVE-2011-0623, CVE-2011-0624, and CVE-2011-0625.
CVE-2011-0627	Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted Flash content, as possibly exploited in the wild in May 2011 by a Microsoft Office document with an embedded .swf file.
CVE-2011-0628	Integer overflow in Adobe Flash Player before 10.3.181.14 on Windows, Mac OS X, Linux, and Solaris and before 10.3.185.21 on Android allows remote attackers to execute arbitrary code via ActionScript that improperly handles a long array object.
CVE-2011-0731	Buffer overflow in the DB2 Administration Server (DAS) component in IBM DB2 9.1 before FP10, 9.5 before FP7, and 9.7 before FP3 on Linux, UNIX, and Windows allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2011-0757	IBM DB2 9.1 before FP10, 9.5 before FP6a, and 9.7 before FP2 on Linux, UNIX, and Windows does not properly revoke the DBADM authority, which allows remote authenticated users to execute non-DDL

	statements by leveraging previous possession of this authority.
CVE-2011-0777	Use-after-free vulnerability in Google Chrome before 9.0.597.84 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to image loading.
CVE-2011-0778	Google Chrome before 9.0.597.84 does not properly restrict drag and drop operations, which might allow remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-0779	Google Chrome before 9.0.597.84 does not properly handle a missing key in an extension, which allows remote attackers to cause a denial of service (application crash) via a crafted extension.
CVE-2011-0780	The PDF event handler in Google Chrome before 9.0.597.84 does not properly interact with print operations, which allows user-assisted remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-0781	Google Chrome before 9.0.597.84 does not properly handle autofill profile merging, which has unspecified impact and remote attack vectors.
CVE-2011-0783	Unspecified vulnerability in Google Chrome before 9.0.597.84 allows user-assisted remote attackers to cause a denial of service (application crash) via vectors involving a "bad volume setting."
CVE-2011-0784	Race condition in Google Chrome before 9.0.597.84 allows remote attackers to execute arbitrary code via vectors related to audio.
CVE-2011-0981	Google Chrome before 9.0.597.94 does not properly perform event handling for animations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-0982	Use-after-free vulnerability in Google Chrome before 9.0.597.94 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG font faces.
CVE-2011-0983	Google Chrome before 9.0.597.94 does not properly handle anonymous blocks, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-0984	Google Chrome before 9.0.597.94 does not properly handle plug-ins, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.

CVE-2011-0985	Google Chrome before 9.0.597.94 does not properly perform process termination upon memory exhaustion, which has unspecified impact and remote attack vectors.
CVE-2011-0994	Stack-based buffer overflow in NFRAgent.exe in Novell File Reporter (NFR) before 1.0.2 allows remote attackers to execute arbitrary code via unspecified XML data.
CVE-2011-1033	Stack-based buffer overflow in oninit in IBM Informix Dynamic Server (IDS) 11.50 allows remote attackers to execute arbitrary code via crafted arguments in the USELASTCOMMITTED session environment option in a SQL SET ENVIRONMENT statement.
CVE-2011-1038	Multiple cross-site scripting (XSS) vulnerabilities in stconf.nsf in the server in IBM Lotus Sametime 8.0.1 allow remote attackers to inject arbitrary web script or HTML via (1) the messageString parameter in a WebMessage action or (2) the PATH_INFO.
CVE-2011-1059	Use-after-free vulnerability in WebCore in WebKit before r77705, as used in Google Chrome before 11.0.672.2 and other products, allows user-assisted remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via vectors that entice a user to resubmit a form, related to improper handling of provisional items by the HistoryController component, aka rdar problem 8938557.
CVE-2011-1106	Cross-site scripting (XSS) vulnerability in stcenter.nsf in the server in IBM Lotus Sametime allows remote attackers to inject arbitrary web script or HTML via the authReasonCode parameter in an OpenDatabase action.
CVE-2011-1107	Unspecified vulnerability in Google Chrome before 9.0.597.107 allows remote attackers to spoof the URL bar via unknown vectors.
CVE-2011-1108	Google Chrome before 9.0.597.107 does not properly implement JavaScript dialogs, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.
CVE-2011-1109	Google Chrome before 9.0.597.107 does not properly process nodes in Cascading Style Sheets (CSS) stylesheets, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1110	Google Chrome before 9.0.597.107 does not properly implement key frame rules, which allows remote attackers to cause a denial of service or possibly have

	unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1111	Google Chrome before 9.0.597.107 does not properly implement forms controls, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1112	Google Chrome before 9.0.597.107 does not properly perform SVG rendering, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1113	Google Chrome before 9.0.597.107 on 64-bit Linux platforms does not properly perform pickle deserialization, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-1114	Google Chrome before 9.0.597.107 does not properly handle tables, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale node."
CVE-2011-1115	Google Chrome before 9.0.597.107 does not properly render tables, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1116	Google Chrome before 9.0.597.107 does not properly handle SVG animations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1117	Google Chrome before 9.0.597.107 does not properly handle XHTML documents, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale nodes."
CVE-2011-1118	Google Chrome before 9.0.597.107 does not properly handle TEXTAREA elements, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document.
CVE-2011-1119	Google Chrome before 9.0.597.107 does not properly determine device orientation, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1120	The WebGL implementation in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial

	of service (out-of-bounds read) via unspecified vectors, aka Issue 71717.
CVE-2011-1121	Integer overflow in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a TEXTAREA element.
CVE-2011-1122	The WebGL implementation in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors, aka Issue 71960.
CVE-2011-1123	Google Chrome before 9.0.597.107 does not properly restrict access to internal extension functions, which has unspecified impact and remote attack vectors.
CVE-2011-1124	Use-after-free vulnerability in Google Chrome before 9.0.597.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to blocked plug-ins.
CVE-2011-1125	Google Chrome before 9.0.597.107 does not properly perform layout, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1185	Google Chrome before 10.0.648.127 does not prevent (1) navigation and (2) close operations on the top location of a sandboxed frame, which has unspecified impact and remote attack vectors.
CVE-2011-1186	Google Chrome before 10.0.648.127 on Linux does not properly handle parallel execution of calls to the print method, which might allow remote attackers to cause a denial of service (application crash) via crafted JavaScript code.
CVE-2011-1187	Google Chrome before 10.0.648.127 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, related to an "error message leak."
CVE-2011-1188	Google Chrome before 10.0.648.127 does not properly handle counter nodes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1189	Google Chrome before 10.0.648.127 does not properly perform box layout, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale node."
CVE-2011-1190	The Web Workers implementation in Google Chrome before 10.0.648.127 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, related to an "error message leak."

CVE-2011-1191	Use-after-free vulnerability in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of DOM URLs.
CVE-2011-1192	Google Chrome before 10.0.648.127 on Linux does not properly handle Unicode ranges, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-1193	Google V8, as used in Google Chrome before 10.0.648.127, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-1194	Multiple unspecified vulnerabilities in Google Chrome before 10.0.648.127 allow remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2011-1195	Use-after-free vulnerability in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to "document script lifetime handling."
CVE-2011-1196	The OGG container implementation in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.
CVE-2011-1197	Google Chrome before 10.0.648.127 does not properly perform table painting, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1198	The video functionality in Google Chrome before 10.0.648.127 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger use of a malformed "out-of-bounds structure."
CVE-2011-1199	Google Chrome before 10.0.648.127 does not properly handle DataView objects, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1200	Google Chrome before 10.0.648.127 does not properly perform a cast of an unspecified variable during text rendering, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2011-1201	The context implementation in WebKit, as used in Google Chrome before 10.0.648.127, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."

CVE-2011-1202	The xsltGenerateIdFunction function in functions.c in libxslt 1.1.26 and earlier, as used in Google Chrome before 10.0.648.127 and other products, allows remote attackers to obtain potentially sensitive information about heap memory addresses via an XML document containing a call to the XSLT generate-id XPath function.
CVE-2011-1203	Google Chrome before 10.0.648.127 does not properly handle SVG cursors, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1204	Google Chrome before 10.0.648.127 does not properly handle attributes, which allows remote attackers to cause a denial of service (DOM tree corruption) or possibly have unspecified other impact via a crafted document.
CVE-2011-1208	IBM solidDB 4.5.x before 4.5.182, 6.0.x before 6.0.1069, 6.1.x and 6.3.x before 6.3 FP8 (aka 6.3.49), and 6.5.x before 6.5 FP4 (aka 6.5.0.4) does not properly handle the (1) rpc_test_svc_readwrite and (2) rpc_test_svc_done commands, which allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted command.
CVE-2011-1285	The regular-expression functionality in Google Chrome before 10.0.648.127 does not properly implement reentrancy, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1286	Google V8, as used in Google Chrome before 10.0.648.127, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger incorrect access to memory.
CVE-2011-1290	Integer overflow in WebKit, as used on the Research In Motion (RIM) BlackBerry Torch 9800 with firmware 6.0.0.246, in Google Chrome before 10.0.648.133, and in Apple Safari before 5.0.5, allows remote attackers to execute arbitrary code via unknown vectors related to CSS "style handling," nodesets, and a length value, as demonstrated by Vincenzo Iozzo, Willem Pinckaers, and Ralf-Philipp Weinmann during a Pwn2Own competition at CanSecWest 2011.
CVE-2011-1291	Google Chrome before 10.0.648.204 does not properly handle base strings, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, related to a "buffer error."

CVE-2011-1292	Use-after-free vulnerability in the frame-loader implementation in Google Chrome before 10.0.648.204 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1293	Use-after-free vulnerability in the HTMLCollection implementation in Google Chrome before 10.0.648.204 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1294	Google Chrome before 10.0.648.204 does not properly handle Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1295	WebKit, as used in Google Chrome before 10.0.648.204 and Apple Safari before 5.0.6, does not properly handle node parentage, which allows remote attackers to cause a denial of service (DOM tree corruption), conduct cross-site scripting (XSS) attacks, or possibly have unspecified other impact via unknown vectors.
CVE-2011-1296	Google Chrome before 10.0.648.204 does not properly handle SVG text, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1301	Use-after-free vulnerability in the GPU process in Google Chrome before 10.0.648.205 allows remote attackers to execute arbitrary code via unknown vectors.
CVE-2011-1302	Heap-based buffer overflow in the GPU process in Google Chrome before 10.0.648.205 allows remote attackers to execute arbitrary code via unknown vectors.
CVE-2011-1303	Google Chrome before 11.0.696.57 does not properly handle floating objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1304	Unspecified vulnerability in Google Chrome before 11.0.696.57 allows remote attackers to bypass the pop-up blocker via vectors related to plug-ins.
CVE-2011-1305	Race condition in Google Chrome before 11.0.696.57 on Linux and Mac OS X allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to linked lists and a database.

CVE-2011-1360	Multiple cross-site scripting (XSS) vulnerabilities in IBM HTTP Server 2.0.47 and earlier, as used in WebSphere Application Server and other products, allow remote attackers to inject arbitrary web script or HTML via vectors involving unspecified documentation files in (1) manual/ibm/ and (2) htdocs/*/manual/ibm/.
CVE-2011-1393	Unspecified vulnerability in the authentication functionality in the server in IBM Lotus Domino 8.x before 8.5.2 FP4 allows remote attackers to cause a denial of service (daemon crash) via a crafted Notes RPC packet.
CVE-2011-1413	Google Chrome before 10.0.648.127 on Linux does not properly mitigate an unspecified flaw in an X server, which allows remote attackers to cause a denial of service (application crash) via vectors involving long messages.
CVE-2011-1434	Google Chrome before 11.0.696.57 does not ensure thread safety during handling of MIME data, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1435	Google Chrome before 11.0.696.57 does not properly implement the tabs permission for extensions, which allows remote attackers to read local files via a crafted extension.
CVE-2011-1436	Google Chrome before 11.0.696.57 on Linux does not properly interact with the X Window System, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2011-1437	Multiple integer overflows in Google Chrome before 11.0.696.57 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to float rendering.
CVE-2011-1438	Google Chrome before 11.0.696.57 allows remote attackers to bypass the Same Origin Policy via vectors involving blobs.
CVE-2011-1439	Google Chrome before 11.0.696.57 on Linux does not properly isolate renderer processes, which has unspecified impact and remote attack vectors.
CVE-2011-1440	Use-after-free vulnerability in Google Chrome before 11.0.696.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the ruby element and Cascading Style Sheets (CSS) token sequences.
CVE-2011-1441	Google Chrome before 11.0.696.57 does not properly perform a cast of an unspecified variable during handling of floating select lists, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted HTML document.

CVE-2011-1442	Google Chrome before 11.0.696.57 does not properly handle mutation events, which allows remote attackers to cause a denial of service (node tree corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1443	Google Chrome before 11.0.696.57 does not properly implement layering, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale pointers."
CVE-2011-1444	Race condition in the sandbox launcher implementation in Google Chrome before 11.0.696.57 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1445	Google Chrome before 11.0.696.57 does not properly handle SVG documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-1446	Google Chrome before 11.0.696.57 allows remote attackers to spoof the URL bar via vectors involving (1) a navigation error or (2) an interrupted load.
CVE-2011-1447	Google Chrome before 11.0.696.57 does not properly handle drop-down lists, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1448	Google Chrome before 11.0.696.57 does not properly perform height calculations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1449	Use-after-free vulnerability in the WebSockets implementation in Google Chrome before 11.0.696.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1450	Google Chrome before 11.0.696.57 does not properly present file dialogs, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "dangling pointers."
CVE-2011-1451	Google Chrome before 11.0.696.57 does not properly handle DOM id maps, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "dangling pointers."

CVE-2011-1452	Google Chrome before 11.0.696.57 allows user-assisted remote attackers to spoof the URL bar via vectors involving a redirect and a manual reload.
CVE-2011-1454	Use-after-free vulnerability in the DOM id handling functionality in Google Chrome before 11.0.696.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted HTML document.
CVE-2011-1455	Google Chrome before 11.0.696.57 does not properly handle PDF documents with multipart encoding, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.
CVE-2011-1456	Google Chrome before 11.0.696.57 does not properly handle PDF forms, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale pointers."
CVE-2011-1465	The SPDY implementation in net/http/http_network_transaction.cc in Google Chrome before 11.0.696.14 drains the bodies from SPDY responses, which might allow remote SPDY servers to cause a denial of service (application exit) by canceling a stream.
CVE-2011-1506	The STARTTLS implementation in Kerio Connect 7.1.4 build 2985 and MailServer 6.x does not properly restrict I/O buffering, which allows man-in-the-middle attackers to insert commands into encrypted SMTP sessions by sending a cleartext command that is processed after TLS is in place, related to a "plaintext command injection" attack, a similar issue to CVE-2011-0411. NOTE: some of these details are obtained from third party information.
CVE-2011-1540	Unspecified vulnerability in HP System Management Homepage (SMH) before 6.3 allows remote authenticated users to execute arbitrary code via unknown vectors.
CVE-2011-1541	Unspecified vulnerability in HP System Management Homepage (SMH) before 6.3 allows remote attackers to bypass intended access restrictions, and consequently execute arbitrary code, via unknown vectors.
CVE-2011-1542	Cross-site scripting (XSS) vulnerability in HP Systems Insight Manager (SIM) before 6.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2011-1543	Cross-site request forgery (CSRF) vulnerability in HP Systems Insight Manager (SIM) before 6.3 allows remote attackers to hijack the authentication of unspecified victims via unknown vectors.

CVE-2011-1560	solid.exe in IBM solidDB before 4.5.181, 6.0.x before 6.0.1067, 6.1.x and 6.3.x before 6.3.47, and 6.5.x before 6.5.0.3 uses a password-hash length specified by the client, which allows remote attackers to bypass authentication via a short length value.
CVE-2011-1691	The counterToCSSValue function in CSSComputedStyleDeclaration.cpp in the Cascading Style Sheets (CSS) implementation in WebCore in WebKit before r82222, as used in Google Chrome before 11.0.696.43 and other products, does not properly handle access to the (1) counterIncrement and (2) counterReset attributes of CSSStyleDeclaration data provided by a getComputedStyle method call, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via crafted JavaScript code.
CVE-2011-1793	rendering/svg/RenderSVGResourceFilter.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted SVG document that leads to a "stale pointer."
CVE-2011-1794	Integer overflow in the FilterEffect::copyImageBytes function in platform/graphics/filters/FilterEffect.cpp in the SVG filter implementation in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted dimensions.
CVE-2011-1795	Integer underflow in the HTMLFormElement::removeFormElement function in html/HTMLFormElement.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted HTML document containing a FORM element.
CVE-2011-1796	Use-after-free vulnerability in the FrameView::calculateScrollbarModesForLayout function in page/FrameView.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code that calls the removeChild method during interaction with a FRAME element.
CVE-2011-1798	rendering/svg/RenderSVGText.cpp in WebCore in WebKit in Google Chrome before 11.0.696.65 does not properly perform a cast of an unspecified variable during an attempt to handle a block child, which allows remote attackers to cause a denial of service (application crash) or possibly have unknown other impact via a crafted text element in an SVG document.

CVE-2011-1799	Google Chrome before 11.0.696.68 does not properly perform casts of variables during interaction with the WebKit engine, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1800	Multiple integer overflows in the SVG Filters implementation in WebCore in WebKit in Google Chrome before 11.0.696.68 allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1801	Unspecified vulnerability in Google Chrome before 11.0.696.71 allows remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2011-1804	rendering/RenderBox.cpp in WebCore in WebKit before r86862, as used in Google Chrome before 11.0.696.71, does not properly render floats, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1806	Google Chrome before 11.0.696.71 does not properly implement the GPU command buffer, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-1807	Google Chrome before 11.0.696.71 does not properly handle blobs, which allows remote attackers to execute arbitrary code via unspecified vectors that trigger an out-of-bounds write.
CVE-2011-1808	Use-after-free vulnerability in Google Chrome before 12.0.742.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to incorrect integer calculations during float handling.
CVE-2011-1809	Use-after-free vulnerability in the accessibility feature in Google Chrome before 12.0.742.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1810	The Cascading Style Sheets (CSS) implementation in Google Chrome before 12.0.742.91 does not properly restrict access to the visit history, which allows remote attackers to obtain sensitive information via unspecified vectors.
CVE-2011-1811	Google Chrome before 12.0.742.91 does not properly handle a large number of form submissions, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2011-1812	Google Chrome before 12.0.742.91 allows remote attackers to bypass intended access restrictions via vectors related to extensions.

CVE-2011-1813	Google Chrome before 12.0.742.91 does not properly implement the framework for extensions, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-1814	Google Chrome before 12.0.742.91 attempts to read data from an uninitialized pointer, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1815	Google Chrome before 12.0.742.91 allows remote attackers to inject script into a tab page via vectors related to extensions.
CVE-2011-1816	Use-after-free vulnerability in the developer tools in Google Chrome before 12.0.742.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1817	Google Chrome before 12.0.742.91 does not properly implement history deletion, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-1818	Use-after-free vulnerability in the image loader in Google Chrome before 12.0.742.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-1819	Google Chrome before 12.0.742.91 allows remote attackers to perform unspecified injection into a chrome:// page via vectors related to extensions.
CVE-2011-1846	IBM DB2 9.5 before FP7 and 9.7 before FP4 on Linux, UNIX, and Windows does not properly revoke role membership from groups, which allows remote authenticated users to execute non-DDL statements by leveraging previous inherited possession of a role, a different vulnerability than CVE-2011-0757. NOTE: some of these details are obtained from third party information.
CVE-2011-1847	IBM DB2 9.5 before FP7 and 9.7 before FP4 on Linux, UNIX, and Windows does not properly enforce privilege requirements for table access, which allows remote authenticated users to modify SYSSTAT.TABLES statistics columns via an UPDATE statement. NOTE: some of these details are obtained from third party information.
CVE-2011-2094	Buffer overflow in Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2095 and CVE-2011-2097.

CVE-2011-2095	Buffer overflow in Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2094 and CVE-2011-2097.
CVE-2011-2096	Heap-based buffer overflow in Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2097	Buffer overflow in Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2094 and CVE-2011-2095.
CVE-2011-2098	Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2099.
CVE-2011-2099	Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2098.
CVE-2011-2100	Untrusted search path vulnerability in Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows allows local users to gain privileges via a Trojan horse DLL in the current working directory.
CVE-2011-2101	Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X do not properly restrict script, which allows attackers to execute arbitrary code via a crafted document, related to a "cross document script execution vulnerability."
CVE-2011-2104	Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allow attackers to cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-2105	Adobe Reader and Acrobat 8.x before 8.3, 9.x before 9.4.5, and 10.x before 10.1 on Windows and Mac OS X allow attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted font data.
CVE-2011-2107	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 10.3.181.22 on Windows, Mac OS X, Linux, and Solaris, and 10.3.185.22 and earlier on Android, allows remote attackers to inject arbitrary web

	script or HTML via unspecified vectors, related to a "universal cross-site scripting vulnerability."
CVE-2011-2110	Adobe Flash Player before 10.3.181.26 on Windows, Mac OS X, Linux, and Solaris, and 10.3.185.23 and earlier on Android, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, as exploited in the wild in June 2011.
CVE-2011-2130	Buffer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2134, CVE-2011-2137, CVE-2011-2414, and CVE-2011-2415.
CVE-2011-2132	Adobe Flash Media Server (FMS) before 3.5.7, and 4.x before 4.0.3, allows attackers to cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-2134	Buffer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2130, CVE-2011-2137, CVE-2011-2414, and CVE-2011-2415.
CVE-2011-2135	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2140, CVE-2011-2417, and CVE-2011-2425.
CVE-2011-2136	Integer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2138 and CVE-2011-2416.
CVE-2011-2137	Buffer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2130, CVE-2011-2134, CVE-2011-2414, and CVE-2011-2415.

CVE-2011-2138	Integer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2136 and CVE-2011-2416.
CVE-2011-2139	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via unspecified vectors.
CVE-2011-2140	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2135, CVE-2011-2417, and CVE-2011-2425.
CVE-2011-2220	Stack-based buffer overflow in NFREngine.exe in Novell File Reporter Engine before 1.0.2.53, as used in Novell File Reporter and other products, allows remote attackers to execute arbitrary code via a crafted RECORD element.
CVE-2011-2332	Google V8, as used in Google Chrome before 12.0.742.91, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-2342	The DOM implementation in Google Chrome before 12.0.742.91 allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-2345	The NPAPI implementation in Google Chrome before 12.0.742.112 does not properly handle strings, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2346	Use-after-free vulnerability in Google Chrome before 12.0.742.112 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG fonts.
CVE-2011-2347	Google Chrome before 12.0.742.112 does not properly handle Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-2348	Google V8, as used in Google Chrome before 12.0.742.112, performs an incorrect bounds check, which allows remote attackers to cause a denial of

	service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2349	Use-after-free vulnerability in Google Chrome before 12.0.742.112 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to text selection.
CVE-2011-2350	The HTML parser in Google Chrome before 12.0.742.112 does not properly address "lifetime and re-entrancy issues," which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2351	Use-after-free vulnerability in Google Chrome before 12.0.742.112 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG use elements.
CVE-2011-2358	Google Chrome before 13.0.782.107 does not ensure that extension installations are confirmed by a browser dialog, which makes it easier for remote attackers to modify the product's functionality via a Trojan horse extension.
CVE-2011-2359	Google Chrome before 13.0.782.107 does not properly track line boxes during rendering, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale pointer."
CVE-2011-2360	Google Chrome before 13.0.782.107 does not ensure that the user is prompted before download of a dangerous file, which makes it easier for remote attackers to bypass intended content restrictions via a crafted web site.
CVE-2011-2361	The Basic Authentication dialog implementation in Google Chrome before 13.0.782.107 does not properly handle strings, which might make it easier for remote attackers to capture credentials via a crafted web site.
CVE-2011-2414	Buffer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2130, CVE-2011-2134, CVE-2011-2137, and CVE-2011-2415.
CVE-2011-2415	Buffer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2130, CVE-2011-2134, CVE-2011-2137, and CVE-2011-2414.

CVE-2011-2416	Integer overflow in Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2136 and CVE-2011-2138.
CVE-2011-2417	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2135, CVE-2011-2140, and CVE-2011-2425.
CVE-2011-2424	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted SWF file, as demonstrated by "about 400 unique crash signatures."
CVE-2011-2425	Adobe Flash Player before 10.3.183.5 on Windows, Mac OS X, Linux, and Solaris and before 10.3.186.3 on Android, and Adobe AIR before 2.7.1 on Windows and Mac OS X and before 2.7.1.1961 on Android, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2135, CVE-2011-2140, and CVE-2011-2417.
CVE-2011-2426	Stack-based buffer overflow in the ActionScript Virtual Machine (AVM) component in Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2427	Stack-based buffer overflow in the ActionScript Virtual Machine (AVM) component in Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows attackers to execute arbitrary code or cause a denial of service via unspecified vectors.
CVE-2011-2428	Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows attackers to execute arbitrary code or cause a denial of service (browser crash) via unspecified vectors, related to a "logic error issue."
CVE-2011-2429	Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7

	on Android, allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors, related to a "security control bypass."
CVE-2011-2430	Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows remote attackers to execute arbitrary code via crafted streaming media, related to a "logic error vulnerability."
CVE-2011-2431	Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allow attackers to execute arbitrary code via unspecified vectors, related to a "security bypass vulnerability."
CVE-2011-2432	Buffer overflow in the U3D TIFF Resource in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2433	Heap-based buffer overflow in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2434 and CVE-2011-2437.
CVE-2011-2434	Heap-based buffer overflow in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2433 and CVE-2011-2437.
CVE-2011-2435	Buffer overflow in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2436	Heap-based buffer overflow in the image-parsing library in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2437	Heap-based buffer overflow in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2011-2433 and CVE-2011-2434.
CVE-2011-2438	Multiple stack-based buffer overflows in the image-parsing library in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allow attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2439	Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allow attackers to execute arbitrary code via unspecified vectors, related to a "memory leakage condition vulnerability."

CVE-2011-2440	Use-after-free vulnerability in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2441	Multiple stack-based buffer overflows in CoolType.dll in Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allow attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2442	Adobe Reader and Acrobat 8.x before 8.3.1, 9.x before 9.4.6, and 10.x before 10.1.1 allow attackers to execute arbitrary code via unspecified vectors, related to a "logic error vulnerability."
CVE-2011-2444	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 10.3.183.10 on Windows, Mac OS X, Linux, and Solaris, and before 10.3.186.7 on Android, allows remote attackers to inject arbitrary web script or HTML via a crafted URL, related to a "universal cross-site scripting issue," as exploited in the wild in September 2011.
CVE-2011-2445	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2451, CVE-2011-2452, CVE-2011-2453, CVE-2011-2454, CVE-2011-2455, CVE-2011-2459, and CVE-2011-2460.
CVE-2011-2450	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via unspecified vectors.
CVE-2011-2451	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2445, CVE-2011-2452, CVE-2011-2453, CVE-2011-2454, CVE-2011-2455, CVE-2011-2459, and CVE-2011-2460.
CVE-2011-2452	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2445, CVE-2011-2451, CVE-2011-2453,

	CVE-2011-2454, CVE-2011-2455, CVE-2011-2459, and CVE-2011-2460.
CVE-2011-2453	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2445, CVE-2011-2451, CVE-2011-2452, CVE-2011-2454, CVE-2011-2455, CVE-2011-2459, and CVE-2011-2460.
CVE-2011-2454	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2445, CVE-2011-2451, CVE-2011-2452, CVE-2011-2453, CVE-2011-2455, CVE-2011-2459, and CVE-2011-2460.
CVE-2011-2455	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2445, CVE-2011-2451, CVE-2011-2452, CVE-2011-2453, CVE-2011-2454, CVE-2011-2459, and CVE-2011-2460.
CVE-2011-2456	Buffer overflow in Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2457	Stack-based buffer overflow in Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-2458	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, when Internet Explorer is used, allows remote attackers to bypass the cross-domain policy via a crafted web site.
CVE-2011-2459	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary

	code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2445, CVE-2011-2451, CVE-2011-2452, CVE-2011-2453, CVE-2011-2454, CVE-2011-2455, and CVE-2011-2460.
CVE-2011-2460	Adobe Flash Player before 10.3.183.11 and 11.x before 11.1.102.55 on Windows, Mac OS X, Linux, and Solaris and before 11.1.102.59 on Android, and Adobe AIR before 3.1.0.4880, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2011-2445, CVE-2011-2451, CVE-2011-2452, CVE-2011-2453, CVE-2011-2454, CVE-2011-2455, and CVE-2011-2459.
CVE-2011-2462	Unspecified vulnerability in the U3D component in Adobe Reader and Acrobat 10.1.1 and earlier on Windows and Mac OS X, and Adobe Reader 9.x through 9.4.6 on UNIX, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, as exploited in the wild in December 2011.
CVE-2011-2463	Cross-site scripting (XSS) vulnerability in Adobe ColdFusion 8.0 through 9.0.1 allows remote attackers to inject arbitrary web script or HTML via vectors involving the cfform tag.
CVE-2011-2474	Directory traversal vulnerability in the HTTP Server in Sybase EAServer 6.3.1 Developer Edition allows remote attackers to read arbitrary files via a /.\..\..\ sequence in a path.
CVE-2011-2750	NFRAgent.exe in Novell File Reporter 1.0.4.2 and earlier allows remote attackers to delete arbitrary files via a full pathname in an SRS OPERATION 4 CMD 5 request to /FSF/CMD.
CVE-2011-2758	IDSWebApp in the Web Administration Tool in IBM Tivoli Directory Server (TDS) 6.2 before 6.2.0.3-TIV-ITDS-IF0004 does not require authentication for access to LDAP Server log files, which allows remote attackers to obtain sensitive information via a crafted URL.
CVE-2011-2759	The login page of IDSWebApp in the Web Administration Tool in IBM Tivoli Directory Server (TDS) 6.2 before 6.2.0.3-TIV-ITDS-IF0004 does not have an off autocomplete attribute for authentication fields, which makes it easier for remote attackers to obtain access by leveraging an unattended workstation.
CVE-2011-2761	Google Chrome 14.0.794.0 does not properly handle a reload of a page generated in response to a POST, which allows user-assisted remote attackers to cause a denial of service (application crash) via a crafted web site, related to GetWidget methods.

CVE-2011-2782	The drag-and-drop implementation in Google Chrome before 13.0.782.107 on Linux does not properly enforce permissions for files, which allows user-assisted remote attackers to bypass intended access restrictions via unspecified vectors.
CVE-2011-2783	Google Chrome before 13.0.782.107 does not ensure that developer-mode NPAPI extension installations are confirmed by a browser dialog, which makes it easier for remote attackers to modify the product's functionality via a Trojan horse extension.
CVE-2011-2784	Google Chrome before 13.0.782.107 allows remote attackers to obtain sensitive information via a request for the GL program log, which reveals a local path in an unspecified log entry.
CVE-2011-2785	The extensions implementation in Google Chrome before 13.0.782.107 does not properly validate the URL for the home page, which allows remote attackers to have an unspecified impact via a crafted extension.
CVE-2011-2786	Google Chrome before 13.0.782.107 does not ensure that the speech-input bubble is shown on the product's screen, which might make it easier for remote attackers to make audio recordings via a crafted web page containing an INPUT element.
CVE-2011-2787	Google Chrome before 13.0.782.107 does not properly address re-entrancy issues associated with the GPU lock, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2011-2788	Buffer overflow in the inspector serialization functionality in Google Chrome before 13.0.782.107 allows user-assisted remote attackers to have an unspecified impact via unknown vectors.
CVE-2011-2789	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to instantiation of the Pepper plug-in.
CVE-2011-2790	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving floating styles.
CVE-2011-2791	The International Components for Unicode (ICU) functionality in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.
CVE-2011-2792	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to float removal.

CVE-2011-2793	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to media selectors.
CVE-2011-2794	Google Chrome before 13.0.782.107 does not properly perform text iteration, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2795	Google Chrome before 13.0.782.107 does not prevent calls to functions in other frames, which allows remote attackers to bypass intended access restrictions via a crafted web site, related to a "cross-frame function leak."
CVE-2011-2796	Use-after-free vulnerability in Skia, as used in Google Chrome before 13.0.782.107, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2797	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to resource caching.
CVE-2011-2798	Google Chrome before 13.0.782.107 does not properly restrict access to internal schemes, which allows remote attackers to have an unspecified impact via a crafted web site.
CVE-2011-2799	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to HTML range handling.
CVE-2011-2800	Google Chrome before 13.0.782.107 allows remote attackers to obtain potentially sensitive information about client-side redirect targets via a crafted web site.
CVE-2011-2801	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the frame loader.
CVE-2011-2802	Google V8, as used in Google Chrome before 13.0.782.107, does not properly perform const lookups, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted web site.
CVE-2011-2803	Google Chrome before 13.0.782.107 does not properly handle Skia paths, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2804	Google Chrome before 13.0.782.107 does not properly handle nested functions in PDF documents, which allows remote attackers to cause a denial of service

	(application crash) or possibly have unspecified other impact via a crafted document.
CVE-2011-2805	Google Chrome before 13.0.782.107 allows remote attackers to bypass the Same Origin Policy and conduct script injection attacks via unspecified vectors.
CVE-2011-2818	Use-after-free vulnerability in Google Chrome before 13.0.782.107 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to display box rendering.
CVE-2011-2819	Google Chrome before 13.0.782.107 allows remote attackers to bypass the Same Origin Policy via vectors related to handling of the base URI.
CVE-2011-2821	Double free vulnerability in libxml2, as used in Google Chrome before 13.0.782.215, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted XPath expression.
CVE-2011-2823	Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a line box.
CVE-2011-2824	Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving counter nodes.
CVE-2011-2825	Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving custom fonts.
CVE-2011-2826	Google Chrome before 13.0.782.215 allows remote attackers to bypass the Same Origin Policy via vectors related to empty origins.
CVE-2011-2827	Use-after-free vulnerability in Google Chrome before 13.0.782.215 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to text searching.
CVE-2011-2828	Google V8, as used in Google Chrome before 13.0.782.215, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.
CVE-2011-2829	Integer overflow in Google Chrome before 13.0.782.215 on 32-bit platforms allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving uniform arrays.
CVE-2011-2830	Google V8, as used in Google Chrome before 14.0.835.163, does not properly implement script object wrappers, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.

CVE-2011-2834	Double free vulnerability in libxml2, as used in Google Chrome before 14.0.835.163, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XPath handling.
CVE-2011-2835	Race condition in Google Chrome before 14.0.835.163 allows attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the certificate cache.
CVE-2011-2836	Google Chrome before 14.0.835.163 does not require Infobar interaction before use of the Windows Media Player plug-in, which makes it easier for remote attackers to have an unspecified impact via crafted Flash content.
CVE-2011-2837	Google Chrome before 14.0.835.163 on Linux does not use the PIC and PIE compiler options for position-independent code, which has unspecified impact and attack vectors.
CVE-2011-2838	Google Chrome before 14.0.835.163 does not properly consider the MIME type during the loading of a plug-in, which has unspecified impact and remote attack vectors.
CVE-2011-2839	The PDF implementation in Google Chrome before 13.0.782.215 on Linux does not properly use the memset library function, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2840	Google Chrome before 14.0.835.163 allows user-assisted remote attackers to spoof the URL bar via vectors related to "unusual user interaction."
CVE-2011-2841	Google Chrome before 14.0.835.163 does not properly perform garbage collection during the processing of PDF documents, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2011-2843	Google Chrome before 14.0.835.163 does not properly handle media buffers, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2844	Google Chrome before 14.0.835.163 does not properly process MP3 files, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2845	Google Chrome before 15.0.874.102 does not properly handle history data, which allows user-assisted remote attackers to spoof the URL bar via unspecified vectors.
CVE-2011-2846	Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial

	of service or possibly have unspecified other impact via vectors related to unload event handling.
CVE-2011-2847	Use-after-free vulnerability in the document loader in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2011-2848	Google Chrome before 14.0.835.163 allows user-assisted remote attackers to spoof the URL bar via vectors related to the forward button.
CVE-2011-2849	The WebSockets implementation in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via unspecified vectors.
CVE-2011-2850	Google Chrome before 14.0.835.163 does not properly handle Khmer characters, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2851	Google Chrome before 14.0.835.163 does not properly handle video, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2852	Off-by-one error in Google V8, as used in Google Chrome before 14.0.835.163, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2853	Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to plug-in handling.
CVE-2011-2854	Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to "ruby / table style handing."
CVE-2011-2855	Google Chrome before 14.0.835.163 does not properly handle Cascading Style Sheets (CSS) token sequences, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to a "stale node."
CVE-2011-2856	Google V8, as used in Google Chrome before 14.0.835.163, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-2857	Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the focus controller.
CVE-2011-2858	Google Chrome before 14.0.835.163 does not properly handle triangle arrays, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.

CVE-2011-2859	Google Chrome before 14.0.835.163 uses incorrect permissions for non-gallery pages, which has unspecified impact and attack vectors.
CVE-2011-2860	Use-after-free vulnerability in Google Chrome before 14.0.835.163 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to table styles.
CVE-2011-2861	Google Chrome before 14.0.835.163 does not properly handle strings in PDF documents, which allows remote attackers to have an unspecified impact via a crafted document that triggers an incorrect read operation.
CVE-2011-2862	Google V8, as used in Google Chrome before 14.0.835.163, does not properly restrict access to built-in objects, which has unspecified impact and remote attack vectors.
CVE-2011-2864	Google Chrome before 14.0.835.163 does not properly handle Tibetan characters, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-2874	Google Chrome before 14.0.835.163 does not perform an expected pin operation for a self-signed certificate during a session, which has unspecified impact and remote attack vectors.
CVE-2011-2875	Google V8, as used in Google Chrome before 14.0.835.163, does not properly perform object sealing, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2011-2876	Use-after-free vulnerability in Google Chrome before 14.0.835.202 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a text line box.
CVE-2011-2877	Google Chrome before 14.0.835.202 does not properly handle SVG text, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that lead to "stale font."
CVE-2011-2878	Google Chrome before 14.0.835.202 does not properly restrict access to the window prototype, which allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2011-2879	Google Chrome before 14.0.835.202 does not properly consider object lifetimes and thread safety during the handling of audio nodes, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-2880	Use-after-free vulnerability in Google Chrome before 14.0.835.202 allows remote attackers to cause a denial

	of service or possibly have unspecified other impact via vectors related to the Google V8 bindings.
CVE-2011-2881	Google Chrome before 14.0.835.202 does not properly handle Google V8 hidden objects, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2011-2903	Heap-based buffer overflow in tcptrack before 1.4.2 might allow attackers to execute arbitrary code via a long command line argument. NOTE: this is only a vulnerability in limited scenarios in which tcptrack is "configured as a handler for other applications." This issue might not qualify for inclusion in CVE.
CVE-2011-3015	Multiple integer overflows in the PDF codecs in Google Chrome before 17.0.963.56 allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3016	Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving counter nodes, related to a "read-after-free" issue.
CVE-2011-3017	Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to database handling.
CVE-2011-3018	Heap-based buffer overflow in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to path rendering.
CVE-2011-3019	Heap-based buffer overflow in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Matroska video (aka MKV) file.
CVE-2011-3020	Unspecified vulnerability in the Native Client validator implementation in Google Chrome before 17.0.963.56 has unknown impact and remote attack vectors.
CVE-2011-3021	Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to subframe loading.
CVE-2011-3022	translate/translate_manager.cc in Google Chrome before 17.0.963.56 and 19.x before 19.0.1036.7 uses an HTTP session to exchange data for translation, which allows remote attackers to obtain sensitive information by sniffing the network.
CVE-2011-3023	Use-after-free vulnerability in Google Chrome before 17.0.963.56 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified

	other impact via vectors related to drag-and-drop operations.
CVE-2011-3024	Google Chrome before 17.0.963.56 allows remote attackers to cause a denial of service (application crash) via an empty X.509 certificate.
CVE-2011-3025	Google Chrome before 17.0.963.56 does not properly parse H.264 data, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3026	Integer overflow in libpng, as used in Google Chrome before 17.0.963.56, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an integer truncation.
CVE-2011-3027	Google Chrome before 17.0.963.56 does not properly perform a cast of an unspecified variable during handling of columns, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2011-3031	Use-after-free vulnerability in the element wrapper in Google V8, as used in Google Chrome before 17.0.963.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3032	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of SVG values.
CVE-2011-3033	Buffer overflow in Skia, as used in Google Chrome before 17.0.963.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3034	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving an SVG document.
CVE-2011-3035	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG use elements.
CVE-2011-3036	Google Chrome before 17.0.963.65 does not properly perform a cast of an unspecified variable during handling of line boxes, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2011-3037	Google Chrome before 17.0.963.65 does not properly perform casts of unspecified variables during the splitting of anonymous blocks, which allows remote

	attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2011-3038	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to multi-column handling.
CVE-2011-3039	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to quote handling.
CVE-2011-3040	Google Chrome before 17.0.963.65 does not properly handle text, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.
CVE-2011-3041	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of class attributes.
CVE-2011-3042	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of table sections.
CVE-2011-3043	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a flexbox (aka flexible box) in conjunction with the floating of elements.
CVE-2011-3044	Use-after-free vulnerability in Google Chrome before 17.0.963.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG animation elements.
CVE-2011-3045	Integer signedness error in the png_inflate function in pngrutil.c in libpng before 1.4.10beta01, as used in Google Chrome before 17.0.963.83 and other products, allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted PNG file, a different vulnerability than CVE-2011-3026.
CVE-2011-3046	The extension subsystem in Google Chrome before 17.0.963.78 does not properly handle history navigation, which allows remote attackers to execute arbitrary code by leveraging a "Universal XSS (UXSS)" issue.
CVE-2011-3047	The GPU process in Google Chrome before 17.0.963.79 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) by leveraging an error in the plug-in loading mechanism.

CVE-2011-3049	Google Chrome before 17.0.963.83 does not properly restrict the extension web request API, which allows remote attackers to cause a denial of service (disrupted system requests) via a crafted extension.
CVE-2011-3050	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 17.0.963.83 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the :first-letter pseudo-element.
CVE-2011-3051	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 17.0.963.83 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the cross-fade function.
CVE-2011-3052	The WebGL implementation in Google Chrome before 17.0.963.83 does not properly handle CANVAS elements, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-3053	Use-after-free vulnerability in Google Chrome before 17.0.963.83 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to block splitting.
CVE-2011-3054	The WebUI privilege implementation in Google Chrome before 17.0.963.83 does not properly perform isolation, which allows remote attackers to bypass intended access restrictions via unspecified vectors.
CVE-2011-3055	The browser native UI in Google Chrome before 17.0.963.83 does not require user confirmation before an unpacked extension installation, which allows user-assisted remote attackers to have an unspecified impact via a crafted extension.
CVE-2011-3056	Google Chrome before 17.0.963.83 allows remote attackers to bypass the Same Origin Policy via vectors involving a "magic iframe."
CVE-2011-3057	Google V8, as used in Google Chrome before 17.0.963.83, allows remote attackers to cause a denial of service via vectors that trigger an invalid read operation.
CVE-2011-3058	Google Chrome before 18.0.1025.142 does not properly handle the EUC-JP encoding system, which might allow remote attackers to conduct cross-site scripting (XSS) attacks via unspecified vectors.
CVE-2011-3059	Google Chrome before 18.0.1025.142 does not properly handle SVG text elements, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3060	Google Chrome before 18.0.1025.142 does not properly handle text fragments, which allows remote

	attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3061	Google Chrome before 18.0.1025.142 does not properly check X.509 certificates before use of a SPDY proxy, which might allow man-in-the-middle attackers to spoof servers or obtain sensitive information via a crafted certificate.
CVE-2011-3062	Off-by-one error in the OpenType Sanitizer in Google Chrome before 18.0.1025.142 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted OpenType file.
CVE-2011-3063	Google Chrome before 18.0.1025.142 does not properly validate the renderer's navigation requests, which has unspecified impact and remote attack vectors.
CVE-2011-3064	Use-after-free vulnerability in Google Chrome before 18.0.1025.142 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG clipping.
CVE-2011-3065	Skia, as used in Google Chrome before 18.0.1025.142, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2011-3066	Skia, as used in Google Chrome before 18.0.1025.151, does not properly perform clipping, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3067	Google Chrome before 18.0.1025.151 allows remote attackers to bypass the Same Origin Policy via vectors related to replacement of IFRAME elements.
CVE-2011-3068	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to run-in boxes.
CVE-2011-3069	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to line boxes.
CVE-2011-3070	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the Google V8 bindings.
CVE-2011-3071	Use-after-free vulnerability in the HTMLMediaElement implementation in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.

CVE-2011-3072	Google Chrome before 18.0.1025.151 allows remote attackers to bypass the Same Origin Policy via vectors related to pop-up windows.
CVE-2011-3073	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of SVG resources.
CVE-2011-3074	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of media.
CVE-2011-3075	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to style-application commands.
CVE-2011-3076	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to focus handling.
CVE-2011-3077	Use-after-free vulnerability in Google Chrome before 18.0.1025.151 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving the script bindings, related to a "read-after-free" issue.
CVE-2011-3078	Use-after-free vulnerability in Google Chrome before 18.0.1025.168 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the floating of elements, a different vulnerability than CVE-2011-3081.
CVE-2011-3079	The Inter-process Communication (IPC) implementation in Google Chrome before 18.0.1025.168, as used in Mozilla Firefox before 38.0 and other products, does not properly validate messages, which has unspecified impact and attack vectors.
CVE-2011-3080	Race condition in the Inter-process Communication (IPC) implementation in Google Chrome before 18.0.1025.168 allows attackers to bypass intended sandbox restrictions via unspecified vectors.
CVE-2011-3081	Use-after-free vulnerability in Google Chrome before 18.0.1025.168 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the floating of elements, a different vulnerability than CVE-2011-3078.
CVE-2011-3083	browser/profiles/profile_impl_io_data.cc in Google Chrome before 19.0.1084.46 does not properly handle a malformed ftp URL in the SRC attribute of a VIDEO element, which allows remote attackers to cause

	a denial of service (NULL pointer dereference and application crash) via a crafted web page.
CVE-2011-3084	Google Chrome before 19.0.1084.46 does not use a dedicated process for the loading of links found on an internal page, which might allow attackers to bypass intended sandbox restrictions via a crafted page.
CVE-2011-3085	The Autofill feature in Google Chrome before 19.0.1084.46 does not properly restrict field values, which allows remote attackers to cause a denial of service (UI corruption) and possibly conduct spoofing attacks via vectors involving long values.
CVE-2011-3086	Use-after-free vulnerability in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a STYLE element.
CVE-2011-3087	Google Chrome before 19.0.1084.46 does not properly perform window navigation, which has unspecified impact and remote attack vectors.
CVE-2011-3088	Google Chrome before 19.0.1084.46 does not properly draw hairlines, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3089	Use-after-free vulnerability in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving tables.
CVE-2011-3090	Race condition in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to worker processes.
CVE-2011-3091	Use-after-free vulnerability in the IndexedDB implementation in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3092	The regex implementation in Google V8, as used in Google Chrome before 19.0.1084.46, allows remote attackers to cause a denial of service (invalid write operation) or possibly have unspecified other impact via unknown vectors.
CVE-2011-3093	Google Chrome before 19.0.1084.46 does not properly handle glyphs, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3094	Google Chrome before 19.0.1084.46 does not properly handle Tibetan text, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.

CVE-2011-3095	The OGG container in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.
CVE-2011-3096	Use-after-free vulnerability in Google Chrome before 19.0.1084.46 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging an error in the GTK implementation of the omnibox.
CVE-2011-3097	The PDF functionality in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging an out-of-bounds write error in the implementation of sampled functions.
CVE-2011-3099	Use-after-free vulnerability in the PDF functionality in Google Chrome before 19.0.1084.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a malformed name for the font encoding.
CVE-2011-3100	Google Chrome before 19.0.1084.46 does not properly draw dash paths, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3101	Google Chrome before 19.0.1084.46 on Linux does not properly mitigate an unspecified flaw in an NVIDIA driver, which has unknown impact and attack vectors. NOTE: see CVE-2012-3105 for the related MFSA 2012-34 issue in Mozilla products.
CVE-2011-3102	Off-by-one error in libxml2, as used in Google Chrome before 19.0.1084.46 and other products, allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via unknown vectors.
CVE-2011-3103	Google V8, as used in Google Chrome before 19.0.1084.52, does not properly perform garbage collection, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2011-3104	Skia, as used in Google Chrome before 19.0.1084.52, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3105	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 19.0.1084.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the :first-letter pseudo-element.
CVE-2011-3106	The WebSockets implementation in Google Chrome before 19.0.1084.52 does not properly handle use of SSL, which allows remote attackers to execute arbitrary

	code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-3107	Google Chrome before 19.0.1084.52 does not properly implement JavaScript bindings for plug-ins, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2011-3108	Use-after-free vulnerability in Google Chrome before 19.0.1084.52 allows remote attackers to execute arbitrary code via vectors related to the browser cache.
CVE-2011-3109	Google Chrome before 19.0.1084.52 on Linux does not properly perform a cast of an unspecified variable, which allows remote attackers to cause a denial of service or possibly have unknown other impact by leveraging an error in the GTK implementation of the UI.
CVE-2011-3110	The PDF functionality in Google Chrome before 19.0.1084.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.
CVE-2011-3111	Google V8, as used in Google Chrome before 19.0.1084.52, allows remote attackers to cause a denial of service (invalid read operation) via unspecified vectors.
CVE-2011-3112	Use-after-free vulnerability in the PDF functionality in Google Chrome before 19.0.1084.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via an invalid encrypted document.
CVE-2011-3113	The PDF functionality in Google Chrome before 19.0.1084.52 does not properly perform a cast of an unspecified variable during handling of color spaces, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2011-3114	Multiple buffer overflows in the PDF functionality in Google Chrome before 19.0.1084.52 allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger unknown function calls.
CVE-2011-3115	Google V8, as used in Google Chrome before 19.0.1084.52, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger "type corruption."
CVE-2011-3234	Google Chrome before 14.0.835.163 does not properly handle boxes, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.

CVE-2011-3388	Opera before 11.51 allows remote attackers to cause an insecure site to appear secure or trusted via unspecified actions related to Extended Validation and loading content from trusted sources in an unspecified sequence that causes the address field and page information dialog to contain security information based on the trusted site, instead of the insecure site.
CVE-2011-3389	The SSL protocol, as used in certain configurations in Microsoft Windows and Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Opera, and other products, encrypts data by using CBC mode with chained initialization vectors, which allows man-in-the-middle attackers to obtain plaintext HTTP headers via a blockwise chosen-boundary attack (BCBA) on an HTTPS session, in conjunction with JavaScript code that uses (1) the HTML5 WebSocket API, (2) the Java URLConnection API, or (3) the Silverlight WebClient API, aka a "BEAST" attack.
CVE-2011-3390	Multiple cross-site scripting (XSS) vulnerabilities in index.php in IBM OpenAdmin Tool (OAT) before 2.72 for Informix allow remote attackers to inject arbitrary web script or HTML via the (1) informixserver, (2) host, or (3) port parameter in a login action.
CVE-2011-3846	Cross-site request forgery (CSRF) vulnerability in HP System Management Homepage (SMH) 6.2.2.7 allows remote attackers to hijack the authentication of administrators for requests that create administrative accounts.
CVE-2011-3873	Google Chrome before 14.0.835.202 does not properly implement shader translation, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-3875	Google Chrome before 15.0.874.102 does not properly handle drag and drop operations on URL strings, which allows user-assisted remote attackers to spoof the URL bar via unspecified vectors.
CVE-2011-3876	Google Chrome before 15.0.874.102 does not properly handle downloading files that have whitespace characters at the end of a filename, which has unspecified impact and user-assisted remote attack vectors.
CVE-2011-3877	Cross-site scripting (XSS) vulnerability in the appcache internals page in Google Chrome before 15.0.874.102 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2011-3878	Race condition in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to worker process initialization.

CVE-2011-3879	Google Chrome before 15.0.874.102 does not prevent redirects to chrome: URLs, which has unspecified impact and remote attack vectors.
CVE-2011-3880	Google Chrome before 15.0.874.102 does not prevent use of an unspecified special character as a delimiter in HTTP headers, which has unknown impact and remote attack vectors.
CVE-2011-3881	WebKit, as used in Google Chrome before 15.0.874.102 and Android before 4.4, allows remote attackers to bypass the Same Origin Policy and conduct Universal XSS (UXSS) attacks via vectors related to (1) the DOMWindow::clear function and use of a selection object, (2) the Object::GetRealNamedPropertyInPrototypeChain function and use of an __proto__ property, (3) the HTMLPlugInImageElement::allowedToLoadFrameURL function and use of a javascript: URL, (4) incorrect origins for XSLT-generated documents in the XSLTProcessor::createDocumentFromSource function, and (5) improper handling of synchronous frame loads in the ScriptController::executeIfJavaScriptURL function.
CVE-2011-3882	Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to media buffers.
CVE-2011-3883	Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to counters.
CVE-2011-3884	Google Chrome before 15.0.874.102 does not properly address timing issues during DOM traversal, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2011-3885	Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to stale Cascading Style Sheets (CSS) token-sequence data.
CVE-2011-3886	Google V8, as used in Google Chrome before 15.0.874.102, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers out-of-bounds write operations.
CVE-2011-3887	Google Chrome before 15.0.874.102 does not properly handle javascript: URLs, which allows remote attackers to bypass intended access restrictions and read cookies via unspecified vectors.

CVE-2011-3888	Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to editing operations in conjunction with an unknown plug-in.
CVE-2011-3889	Heap-based buffer overflow in the Web Audio implementation in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3890	Use-after-free vulnerability in Google Chrome before 15.0.874.102 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to video source handling.
CVE-2011-3891	Google Chrome before 15.0.874.102 does not properly restrict access to internal Google V8 functions, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3892	Double free vulnerability in the Theora decoder in Google Chrome before 15.0.874.120 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted stream.
CVE-2011-3893	Google Chrome before 15.0.874.120 does not properly implement the MKV and Vorbis media handlers, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3894	Google Chrome before 15.0.874.120 does not properly perform VP8 decoding, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted stream.
CVE-2011-3895	Heap-based buffer overflow in the Vorbis decoder in Google Chrome before 15.0.874.120 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted stream.
CVE-2011-3896	Buffer overflow in Google Chrome before 15.0.874.120 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to shader variable mapping.
CVE-2011-3897	Use-after-free vulnerability in Google Chrome before 15.0.874.120 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to editing.
CVE-2011-3898	Google Chrome before 15.0.874.120, when Java Runtime Environment (JRE) 7 is used, does not request user confirmation before applet execution begins, which allows remote attackers to have an unspecified impact via a crafted applet.

CVE-2011-3900	Google V8, as used in Google Chrome before 15.0.874.121, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write operation.
CVE-2011-3903	Google Chrome before 16.0.912.63 does not properly perform regex matching, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3904	Use-after-free vulnerability in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to bidirectional text (aka bidi) handling.
CVE-2011-3905	libxml2, as used in Google Chrome before 16.0.912.63, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3906	The PDF parser in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3907	The view-source feature in Google Chrome before 16.0.912.63 allows remote attackers to spoof the URL bar via unspecified vectors.
CVE-2011-3908	Google Chrome before 16.0.912.63 does not properly parse SVG documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3909	The Cascading Style Sheets (CSS) implementation in Google Chrome before 16.0.912.63 on 64-bit platforms does not properly manage property arrays, which allows remote attackers to cause a denial of service (memory corruption) via unspecified vectors.
CVE-2011-3910	Google Chrome before 16.0.912.63 does not properly handle YUV video frames, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3911	Google Chrome before 16.0.912.63 does not properly handle PDF documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3912	Use-after-free vulnerability in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG filters.
CVE-2011-3913	Use-after-free vulnerability in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to Range handling.
CVE-2011-3914	The internationalization (aka i18n) functionality in Google V8, as used in Google Chrome before

	16.0.912.63, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors that trigger an out-of-bounds write.
CVE-2011-3915	Buffer overflow in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to PDF fonts.
CVE-2011-3916	Google Chrome before 16.0.912.63 does not properly handle PDF cross references, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3917	Stack-based buffer overflow in FileWatcher in Google Chrome before 16.0.912.63 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3919	Heap-based buffer overflow in libxml2, as used in Google Chrome before 16.0.912.75, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3921	Use-after-free vulnerability in Google Chrome before 16.0.912.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving animation frames.
CVE-2011-3922	Stack-based buffer overflow in Google Chrome before 16.0.912.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to glyph handling.
CVE-2011-3924	Use-after-free vulnerability in Google Chrome before 16.0.912.77 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOM selections.
CVE-2011-3925	Use-after-free vulnerability in the Safe Browsing feature in Google Chrome before 16.0.912.75 allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact via vectors related to a navigation entry and an interstitial page.
CVE-2011-3926	Heap-based buffer overflow in the tree builder in Google Chrome before 16.0.912.77 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3927	Skia, as used in Google Chrome before 16.0.912.77, does not perform all required initialization of values, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3928	Use-after-free vulnerability in Google Chrome before 16.0.912.77 allows remote attackers to cause a denial

	of service or possibly have unspecified other impact via vectors related to DOM handling.
CVE-2011-3953	Google Chrome before 17.0.963.46 does not prevent monitoring of the clipboard after a paste event, which has unspecified impact and remote attack vectors.
CVE-2011-3954	Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (application crash) via vectors that trigger a large amount of database usage.
CVE-2011-3955	Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via vectors that trigger the aborting of an IndexedDB transaction.
CVE-2011-3956	The extension implementation in Google Chrome before 17.0.963.46 does not properly handle sandboxed origins, which might allow remote attackers to bypass the Same Origin Policy via a crafted extension.
CVE-2011-3957	Use-after-free vulnerability in the garbage-collection functionality in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving PDF documents.
CVE-2011-3958	Google Chrome before 17.0.963.46 does not properly perform casts of variables during handling of a column span, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2011-3959	Buffer overflow in the locale implementation in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2011-3960	Google Chrome before 17.0.963.46 does not properly decode audio data, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3961	Race condition in Google Chrome before 17.0.963.46 allows remote attackers to execute arbitrary code via vectors that trigger a crash of a utility process.
CVE-2011-3962	Google Chrome before 17.0.963.46 does not properly perform path clipping, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3963	Google Chrome before 17.0.963.46 does not properly handle PDF FAX images, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.

CVE-2011-3964	Google Chrome before 17.0.963.46 does not properly implement the drag-and-drop feature, which makes it easier for remote attackers to spoof the URL bar via unspecified vectors.
CVE-2011-3965	Google Chrome before 17.0.963.46 does not properly check signatures, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2011-3966	Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to error handling for Cascading Style Sheets (CSS) token-sequence data.
CVE-2011-3967	Unspecified vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (application crash) via a crafted certificate.
CVE-2011-3968	Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving Cascading Style Sheets (CSS) token sequences.
CVE-2011-3969	Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to layout of SVG documents.
CVE-2011-3970	libxslt, as used in Google Chrome before 17.0.963.46, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-3971	Use-after-free vulnerability in Google Chrome before 17.0.963.46 allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to mousemove events.
CVE-2011-3972	The shader translator implementation in Google Chrome before 17.0.963.46 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2011-4368	Cross-site scripting (XSS) vulnerability in Remote Development Services (RDS) in Adobe ColdFusion 8.0 through 9.0.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2011-4369	Unspecified vulnerability in the PRC component in Adobe Reader and Acrobat 9.x before 9.4.7 on Windows, Adobe Reader and Acrobat 9.x through 9.4.6 on Mac OS X, Adobe Reader and Acrobat 10.x through 10.1.1 on Windows and Mac OS X, and Adobe Reader 9.x through 9.4.6 on UNIX allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unknown vectors, as exploited in the wild in December 2011.

CVE-2011-4374	Integer overflow in Adobe Reader 9.x before 9.4.6 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2011-4681	Opera before 11.60 does not properly consider the number of . (dot) characters that conventionally exist in domain names of different top-level domains, which allows remote attackers to bypass the Same Origin Policy by leveraging access to a different domain name in the same top-level domain, as demonstrated by the .no or .uk domain.
CVE-2011-4682	The JavaScript engine in Opera before 11.60 does not properly implement the in operator, which allows remote attackers to bypass the Same Origin Policy via vectors related to variables on different web sites.
CVE-2011-4683	Unspecified vulnerability in Opera before 11.60 has unknown impact and attack vectors, related to a "moderately severe issue."
CVE-2011-4684	Opera before 11.60 does not properly handle certificate revocation, which has unspecified impact and remote attack vectors related to "corner cases."
CVE-2011-4685	Dragonfly in Opera before 11.60 allows remote attackers to cause a denial of service (application crash) via unspecified content on a web page, as demonstrated by forbes.com.
CVE-2011-4686	Unspecified vulnerability in the Web Workers implementation in Opera before 11.60 allows remote attackers to cause a denial of service (application crash) via unknown vectors.
CVE-2011-4687	Opera before 11.60 allows remote attackers to cause a denial of service (CPU and memory consumption) via unspecified content on a web page, as demonstrated by a page under the cisco.com home page.
CVE-2011-4690	Opera 11.60 and earlier does not prevent capture of data about the times of Same Origin Policy violations during IFRAME loading attempts, which makes it easier for remote attackers to determine whether a document exists in the browser cache via crafted JavaScript code.
CVE-2011-4691	Google Chrome 15.0.874.121 and earlier does not prevent capture of data about the times of Same Origin Policy violations during IFRAME loading attempts, which makes it easier for remote attackers to determine whether a document exists in the browser cache via crafted JavaScript code.
CVE-2011-4692	WebKit, as used in Apple Safari 5.1.1 and earlier and Google Chrome 15 and earlier, does not prevent capture of data about the time required for image loading, which makes it easier for remote attackers to determine whether an image exists in the browser

	cache via crafted JavaScript code, as demonstrated by visipisi.
CVE-2011-4708	Cross-site scripting (XSS) vulnerability in IBM Rational Asset Manager before 7.5.1 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2011-4800	Directory traversal vulnerability in Serv-U FTP Server before 11.1.0.5 allows remote authenticated users to read and write arbitrary files, and list and create arbitrary directories, via a "..:/" (dot dot colon forward slash) in the (1) list, (2) put, or (3) get commands.
CVE-2011-4890	The server in IBM solidDB 6.5 before FP9 and 7.0 before FP1 allows remote authenticated users to cause a denial of service (daemon crash) via a SELECT statement with a ROWNUM condition involving a subquery.
CVE-2011-5319	content/renderer/device_sensors/device_motion_event_pump.cc in Google Chrome before 41.0.2272.76 does not properly restrict access to high-rate accelerometer data, which makes it easier for remote attackers to capture keystrokes via a crafted web site that listens for ondevicemotion events, a different vulnerability than CVE-2015-1231.
CVE-2011-5326	imlib2 before 1.4.9 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) by drawing a 2x1 ellipse.
CVE-2012-0135	Unspecified vulnerability in HP System Management Homepage (SMH) before 7.0 allows remote authenticated users to cause a denial of service via unknown vectors.
CVE-2012-0200	The server in IBM solidDB 6.5 before Interim Fix 6 does not properly initialize data structures, which allows remote authenticated users to cause a denial of service (daemon crash) via a SELECT statement with a redundant WHERE condition.
CVE-2012-0307	Multiple cross-site scripting (XSS) vulnerabilities in Symantec Messaging Gateway (SMG) before 10.0 allow remote attackers to inject arbitrary web script or HTML via (1) web content or (2) e-mail content.
CVE-2012-0308	Cross-site request forgery (CSRF) vulnerability in Symantec Messaging Gateway (SMG) before 10.0 allows remote attackers to hijack the authentication of administrators.
CVE-2012-0409	Multiple buffer overflows in EMC AutoStart 5.3.x and 5.4.x before 5.4.3 allow remote attackers to cause a denial of service (agent crash) or possibly execute arbitrary code via crafted packets.
CVE-2012-0428	Cross-site scripting (XSS) vulnerability in NetIQ eDirectory 8.8.6.x before 8.8.6.7 and 8.8.7.x before

	8.8.7.2 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2012-0432	Stack-based buffer overflow in the Novell NCP implementation in NetIQ eDirectory 8.8.7.x before 8.8.7.2 allows remote attackers to have an unspecified impact via unknown vectors.
CVE-2012-0691	CA License (aka CA Licensing) before 1.90.03 does not properly restrict system commands, which allows local users to gain privileges via unspecified vectors.
CVE-2012-0692	CA License (aka CA Licensing) before 1.90.03 allows local users to modify or create arbitrary files, and consequently gain privileges, via unspecified vectors.
CVE-2012-0709	IBM DB2 9.5 before FP9, 9.7 through FP5, and 9.8 through FP4 does not properly check variables, which allows remote authenticated users to bypass intended restrictions on viewing table data by leveraging the CREATEIN privilege to execute crafted SQL CREATE VARIABLE statements.
CVE-2012-0710	IBM DB2 9.1 before FP11, 9.5 before FP9, 9.7 before FP5, and 9.8 before FP4 allows remote attackers to cause a denial of service (daemon crash) via a crafted Distributed Relational Database Architecture (DRDA) request.
CVE-2012-0711	Integer signedness error in the db2dasrrm process in the DB2 Administration Server (DAS) in IBM DB2 9.1 through FP11, 9.5 before FP9, and 9.7 through FP5 on UNIX platforms allows remote attackers to execute arbitrary code via a crafted request that triggers a heap-based buffer overflow.
CVE-2012-0712	The XML feature in IBM DB2 9.5 before FP9, 9.7 through FP5, and 9.8 through FP4 allows remote authenticated users to cause a denial of service (infinite loop) by calling the XMLPARSE function with a crafted string expression.
CVE-2012-0713	Unspecified vulnerability in the XML feature in IBM DB2 9.7 before FP6 on Linux, UNIX, and Windows allows remote authenticated users to read arbitrary XML files via unknown vectors.
CVE-2012-0724	Adobe Flash Player before 11.2.202.229 in Google Chrome before 18.0.1025.151 allow attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2012-0725.
CVE-2012-0725	Adobe Flash Player before 11.2.202.229 in Google Chrome before 18.0.1025.151 allow attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2012-0724.

CVE-2012-0726	The default configuration of TLS in IBM Tivoli Directory Server (TDS) 6.3 and earlier supports the (1) NULL-MD5 and (2) NULL-SHA ciphers, which allows remote attackers to trigger unencrypted communication via the TLS Handshake Protocol.
CVE-2012-0740	Cross-site scripting (XSS) vulnerability in the Web Admin Tool in IBM Tivoli Directory Server (TDS) 6.2 before 6.2.0.22 and 6.3 before 6.3.0.11 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2012-0743	IBM Tivoli Directory Server (TDS) 6.3 and earlier allows remote attackers to cause a denial of service (daemon crash) via a malformed LDAP paged search request.
CVE-2012-0752	Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to execute arbitrary code or cause a denial of service (memory corruption) by leveraging an unspecified "type confusion."
CVE-2012-0753	Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted MP4 data.
CVE-2012-0754	Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2012-0755	Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2012-0756.
CVE-2012-0756	Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2012-0755.
CVE-2012-0767	Cross-site scripting (XSS) vulnerability in Adobe Flash Player before 10.3.183.15 and 11.x before 11.1.102.62 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.6 on Android 2.x and 3.x; and before 11.1.115.6 on Android 4.x allows remote attackers to inject arbitrary web script or HTML via

	unspecified vectors, aka "Universal XSS (UXSS)," as exploited in the wild in February 2012.
CVE-2012-0768	The Matrix3D component in Adobe Flash Player before 10.3.183.16 and 11.x before 11.1.102.63 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.7 on Android 2.x and 3.x; and before 11.1.115.7 on Android 4.x allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2012-0769	Adobe Flash Player before 10.3.183.16 and 11.x before 11.1.102.63 on Windows, Mac OS X, Linux, and Solaris; before 11.1.111.7 on Android 2.x and 3.x; and before 11.1.115.7 on Android 4.x does not properly handle integers, which allows attackers to obtain sensitive information via unspecified vectors.
CVE-2012-0770	Adobe ColdFusion 8.0, 8.0.1, 9.0, and 9.0.1 computes hash values for form parameters without restricting the ability to trigger hash collisions predictably, which allows remote attackers to cause a denial of service (CPU consumption) by sending many crafted parameters.
CVE-2012-0773	The NetStream class in Adobe Flash Player before 10.3.183.18 and 11.x before 11.2.202.228 on Windows, Mac OS X, and Linux; Flash Player before 10.3.183.18 and 11.x before 11.2.202.223 on Solaris; Flash Player before 11.1.111.8 on Android 2.x and 3.x; and AIR before 3.2.0.2070 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2012-0774	Integer overflow in Adobe Reader and Acrobat 9.x before 9.5.1 and 10.x before 10.1.3 allows attackers to execute arbitrary code via a crafted TrueType font.
CVE-2012-0775	The JavaScript implementation in Adobe Reader and Acrobat 9.x before 9.5.1 and 10.x before 10.1.3 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2012-0776	The installer in Adobe Reader 9.x before 9.5.1 and 10.x before 10.1.3 allows attackers to bypass intended access restrictions and execute arbitrary code via unspecified vectors.
CVE-2012-0777	The JavaScript API in Adobe Reader and Acrobat 9.x before 9.5.1 and 10.x before 10.1.3 on Mac OS X and Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2012-0779	Adobe Flash Player before 10.3.183.19 and 11.x before 11.2.202.235 on Windows, Mac OS X, and Linux; before 11.1.111.9 on Android 2.x and 3.x; and before 11.1.115.8 on Android 4.x allows remote attackers to execute arbitrary code via a crafted file, related to an

	"object confusion vulnerability," as exploited in the wild in May 2012.
CVE-2012-1003	Multiple integer overflows in Opera 11.60 and earlier allow remote attackers to cause a denial of service (application crash) via a large integer argument to the (1) Int32Array, (2) Float32Array, (3) Float64Array, (4) Uint32Array, (5) Int16Array, or (6) ArrayBuffer function. NOTE: the vendor reportedly characterizes this as "a stability issue, not a security issue."
CVE-2012-1251	Opera before 9.63 does not properly verify X.509 certificates from SSL servers, which allows man-in-the-middle attackers to spoof servers and obtain sensitive information via a crafted certificate.
CVE-2012-1521	Use-after-free vulnerability in the XML parser in Google Chrome before 18.0.1025.168 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-1530	Heap-based buffer overflow in the XSLT engine in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via a PDF file containing an XSL file that triggers memory corruption when the lang function processes XML data with a crafted node-set.
CVE-2012-1535	Unspecified vulnerability in Adobe Flash Player before 11.3.300.271 on Windows and Mac OS X and before 11.2.202.238 on Linux allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via crafted SWF content, as exploited in the wild in August 2012 with SWF content in a Word document.
CVE-2012-1796	Unspecified vulnerability in IBM Tivoli Monitoring Agent (ITMA), as used in IBM DB2 9.5 before FP9 on UNIX, allows local users to gain privileges via unknown vectors.
CVE-2012-1797	IBM DB2 9.5 uses world-writable permissions for nodes.reg, which has unspecified impact and attack vectors.
CVE-2012-1845	Use-after-free vulnerability in Google Chrome 17.0.963.66 and earlier allows remote attackers to bypass the DEP and ASLR protection mechanisms, and execute arbitrary code, via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2012. NOTE: the primary affected product may be clarified later; it was not identified by the researcher, who reportedly stated "it really doesn't matter if it's third-party code."
CVE-2012-1846	Google Chrome 17.0.963.66 and earlier allows remote attackers to bypass the sandbox protection mechanism by leveraging access to a sandboxed process,

	as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2012. NOTE: the primary affected product may be clarified later; it was not identified by the researcher, who reportedly stated "it really doesn't matter if it's third-party code."
CVE-2012-1908	Cross-site scripting (XSS) vulnerability in Splunk 4.0 through 4.3 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.
CVE-2012-1924	Opera before 11.62 allows user-assisted remote attackers to trick users into downloading and executing arbitrary files via a small window for the download dialog.
CVE-2012-1925	Opera before 11.62 does not ensure that a dialog window is placed on top of content windows, which makes it easier for user-assisted remote attackers to trick users into downloading and executing arbitrary files via a download dialog located under other windows.
CVE-2012-1926	Opera before 11.62 allows remote attackers to bypass the Same Origin Policy via the (1) history.pushState and (2) history.replaceState functions in conjunction with cross-domain frames, leading to unintended read access to history.state information.
CVE-2012-1927	Opera before 11.62 allows remote attackers to spoof the address field by triggering the launch of a dialog window associated with a different domain.
CVE-2012-1928	Opera before 11.62 allows remote attackers to spoof the address field by triggering a page reload followed by a redirect to a different domain.
CVE-2012-1930	Opera before 11.62 on UNIX uses world-readable permissions for temporary files during printing, which allows local users to obtain sensitive information by reading these files.
CVE-2012-1931	Opera before 11.62 on UNIX, when used in conjunction with an unspecified printing application, allows local users to overwrite arbitrary files via a symlink attack on a temporary file during printing.
CVE-2012-1993	Unspecified vulnerability in HP System Management Homepage (SMH) before 7.0 allows local users to modify data or obtain sensitive information via unknown vectors.
CVE-2012-2000	Multiple unspecified vulnerabilities in HP System Health Application and Command Line Utilities before 9.0.0 allow remote attackers to execute arbitrary code via unknown vectors.
CVE-2012-2001	Cross-site scripting (XSS) vulnerability in HP SNMP Agents for Linux before 9.0.0 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

CVE-2012-2002	Open redirect vulnerability in HP SNMP Agents for Linux before 9.0.0 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.
CVE-2012-2012	HP System Management Homepage (SMH) before 7.1.1 does not have an off autocomplete attribute for unspecified form fields, which makes it easier for remote attackers to obtain access by leveraging an unattended workstation.
CVE-2012-2013	Unspecified vulnerability in HP System Management Homepage (SMH) before 7.1.1 allows remote attackers to cause a denial of service, or possibly obtain sensitive information or modify data, via unknown vectors.
CVE-2012-2014	HP System Management Homepage (SMH) before 7.1.1 does not properly validate input, which allows remote authenticated users to have an unspecified impact via unknown vectors.
CVE-2012-2015	Unspecified vulnerability in HP System Management Homepage (SMH) before 7.1.1 allows remote authenticated users to gain privileges and obtain sensitive information via unknown vectors.
CVE-2012-2016	Unspecified vulnerability in HP System Management Homepage (SMH) before 7.1.1 allows local users to obtain sensitive information via unknown vectors.
CVE-2012-2034	Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X; before 10.3.183.20 and 11.x before 11.2.202.236 on Linux; before 11.1.111.10 on Android 2.x and 3.x; and before 11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-2037.
CVE-2012-2035	Stack-based buffer overflow in Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X; before 10.3.183.20 and 11.x before 11.2.202.236 on Linux; before 11.1.111.10 on Android 2.x and 3.x; and before 11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows attackers to execute arbitrary code via unspecified vectors.
CVE-2012-2036	Integer overflow in Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X; before 10.3.183.20 and 11.x before 11.2.202.236 on Linux; before 11.1.111.10 on Android 2.x and 3.x; and before 11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows attackers to execute arbitrary code via unspecified vectors.
CVE-2012-2037	Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X; before 10.3.183.20 and 11.x before 11.2.202.236 on

	Linux; before 11.1.111.10 on Android 2.x and 3.x; and before 11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-2034.
CVE-2012-2038	Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X; before 10.3.183.20 and 11.x before 11.2.202.236 on Linux; before 11.1.111.10 on Android 2.x and 3.x; and before 11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors.
CVE-2012-2039	Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X; before 10.3.183.20 and 11.x before 11.2.202.236 on Linux; before 11.1.111.10 on Android 2.x and 3.x; and before 11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows attackers to execute arbitrary code or cause a denial of service (NULL pointer dereference) via unspecified vectors.
CVE-2012-2040	Untrusted search path vulnerability in the installer in Adobe Flash Player before 10.3.183.20 and 11.x before 11.3.300.257 on Windows and Mac OS X; before 10.3.183.20 and 11.x before 11.2.202.236 on Linux; before 11.1.111.10 on Android 2.x and 3.x; and before 11.1.115.9 on Android 4.x, and Adobe AIR before 3.3.0.3610, allows local users to gain privileges via a Trojan horse executable file in an unspecified directory.
CVE-2012-2041	CRLF injection vulnerability in the Component Browser in Adobe ColdFusion 8.0 through 9.0.1 allows remote attackers to inject arbitrary HTTP headers and conduct HTTP response splitting attacks via unspecified vectors.
CVE-2012-2048	Unspecified vulnerability in Adobe ColdFusion 10 and earlier allows attackers to cause a denial of service via unknown vectors.
CVE-2012-2174	The URL handler in IBM Lotus Notes 8.x before 8.5.3 FP2 allows remote attackers to execute arbitrary code via a crafted notes:// URL.
CVE-2012-2180	The chaining functionality in the Distributed Relational Database Architecture (DRDA) module in IBM DB2 9.7 before FP6 and 9.8 before FP5 allows remote attackers to cause a denial of service (NULL pointer dereference, and resource consumption or daemon crash) via a crafted request.
CVE-2012-2194	Directory traversal vulnerability in the SQLJ.DB2_INSTALL_JAR stored procedure in IBM DB2 9.1 before FP12, 9.5 through FP9, 9.7 through

	FP6, 9.8 through FP5, and 10.1 allows remote attackers to replace JAR files via unspecified vectors.
CVE-2012-2196	IBM DB2 9.1 before FP12, 9.5 through FP9, 9.7 through FP6, 9.8 through FP5, and 10.1 allows remote attackers to read arbitrary XML files via the (1) GET_WRAP_CFG_C or (2) GET_WRAP_CFG_C2 stored procedure.
CVE-2012-2197	Stack-based buffer overflow in the Java Stored Procedure infrastructure in IBM DB2 9.1 before FP12, 9.5 through FP9, 9.7 through FP6, 9.8 through FP5, and 10.1 allows remote authenticated users to execute arbitrary code by leveraging certain CONNECT and EXECUTE privileges.
CVE-2012-2807	Multiple integer overflows in libxml2, as used in Google Chrome before 20.0.1132.43 and other products, on 64-bit Linux platforms allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-2815	Google Chrome before 20.0.1132.43 allows remote attackers to obtain potentially sensitive information from a fragment identifier by leveraging access to an IFRAME element associated with a different domain.
CVE-2012-2817	Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to tables that have sections.
CVE-2012-2818	Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the layout of documents that use the Cascading Style Sheets (CSS) counters feature.
CVE-2012-2819	The texSubImage2D implementation in the WebGL subsystem in Google Chrome before 20.0.1132.43 does not properly handle uploads to floating-point textures, which allows remote attackers to cause a denial of service (assertion failure and application crash) or possibly have unspecified other impact via a crafted web page, as demonstrated by certain WebGL performance tests, aka rdar problem 11520387.
CVE-2012-2820	Google Chrome before 20.0.1132.43 does not properly implement SVG filters, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-2821	The autofill implementation in Google Chrome before 20.0.1132.43 does not properly display text, which has unspecified impact and remote attack vectors.
CVE-2012-2822	The PDF functionality in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.

CVE-2012-2823	Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG resources.
CVE-2012-2824	Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG painting.
CVE-2012-2825	The XSL implementation in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service (incorrect read operation) via unspecified vectors.
CVE-2012-2826	Google Chrome before 20.0.1132.43 does not properly implement texture conversion, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-2828	Multiple integer overflows in the PDF functionality in Google Chrome before 20.0.1132.43 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2829	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the :first-letter pseudo-element.
CVE-2012-2830	Google Chrome before 20.0.1132.43 does not properly set array values, which allows remote attackers to cause a denial of service (incorrect pointer use) or possibly have unspecified other impact via unknown vectors.
CVE-2012-2831	Use-after-free vulnerability in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG references.
CVE-2012-2832	The image-codec implementation in the PDF functionality in Google Chrome before 20.0.1132.43 does not initialize an unspecified pointer, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2012-2833	Buffer overflow in the JS API in the PDF functionality in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-2834	Integer overflow in Google Chrome before 20.0.1132.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted data in the Matroska container format.

CVE-2012-2842	Use-after-free vulnerability in Google Chrome before 20.0.1132.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to counter handling.
CVE-2012-2843	Use-after-free vulnerability in Google Chrome before 20.0.1132.57 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to layout height tracking.
CVE-2012-2844	The PDF functionality in Google Chrome before 20.0.1132.57 does not properly handle JavaScript code, which allows remote attackers to cause a denial of service (incorrect object access) or possibly have unspecified other impact via a crafted document.
CVE-2012-2846	Google Chrome before 21.0.1180.57 on Linux does not properly isolate renderer processes, which allows remote attackers to cause a denial of service (cross-process interference) via unspecified vectors.
CVE-2012-2847	Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, does not request user confirmation before continuing a large series of downloads, which allows user-assisted remote attackers to cause a denial of service (resource consumption) via a crafted web site.
CVE-2012-2848	The drag-and-drop implementation in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows user-assisted remote attackers to bypass intended file access restrictions via a crafted web site.
CVE-2012-2849	Off-by-one error in the GIF decoder in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted image.
CVE-2012-2850	Multiple unspecified vulnerabilities in the PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allow remote attackers to have an unknown impact via a crafted document.
CVE-2012-2851	Multiple integer overflows in the PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2852	The PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, does not properly handle object linkage, which allows remote attackers to cause a denial of service (use-after-free)

	or possibly have unspecified other impact via a crafted document.
CVE-2012-2853	The webRequest API in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, does not properly interact with the Chrome Web Store, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site.
CVE-2012-2854	Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to obtain potentially sensitive information about pointer values by leveraging access to a WebUI renderer process.
CVE-2012-2855	Use-after-free vulnerability in the PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2856	The PDF functionality in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.
CVE-2012-2857	Use-after-free vulnerability in the Cascading Style Sheets (CSS) DOM implementation in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2858	Buffer overflow in the WebP decoder in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted WebP image.
CVE-2012-2859	Google Chrome before 21.0.1180.57 on Linux does not properly handle tabs, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors.
CVE-2012-2860	The date-picker implementation in Google Chrome before 21.0.1180.57 on Mac OS X and Linux, and before 21.0.1180.60 on Windows and Chrome Frame, allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site.

CVE-2012-2862	Use-after-free vulnerability in the PDF functionality in Google Chrome before 21.0.1180.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2863	The PDF functionality in Google Chrome before 21.0.1180.75 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.
CVE-2012-2865	Google Chrome before 21.0.1180.89 does not properly perform line breaking, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.
CVE-2012-2866	Google Chrome before 21.0.1180.89 does not properly perform a cast of an unspecified variable during handling of run-in elements, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2012-2867	The SPDY implementation in Google Chrome before 21.0.1180.89 allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2012-2868	Race condition in Google Chrome before 21.0.1180.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving improper interaction between worker processes and an XMLHttpRequest (aka XHR) object.
CVE-2012-2869	Google Chrome before 21.0.1180.89 does not properly load URLs, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a "stale buffer."
CVE-2012-2870	libxslt 1.1.26 and earlier, as used in Google Chrome before 21.0.1180.89, does not properly manage memory, which might allow remote attackers to cause a denial of service (application crash) via a crafted XSLT expression that is not properly identified during XPath navigation, related to (1) the xsltCompileLocationPathPattern function in libxslt/pattern.c and (2) the xsltGenerateIdFunction function in libxslt/functions.c.
CVE-2012-2871	libxml2 2.9.0-rc1 and earlier, as used in Google Chrome before 21.0.1180.89, does not properly support a cast of an unspecified variable during handling of XSL transforms, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document, related to the _xmlNs data structure in include/libxml/tree.h.
CVE-2012-2872	Cross-site scripting (XSS) vulnerability in an SSL interstitial page in Google Chrome before 21.0.1180.89 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.

CVE-2012-2874	Skia, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an out-of-bounds write operation, a different vulnerability than CVE-2012-2883.
CVE-2012-2875	Multiple unspecified vulnerabilities in the PDF functionality in Google Chrome before 22.0.1229.79 allow remote attackers to have an unknown impact via a crafted document.
CVE-2012-2876	Buffer overflow in the SSE2 optimization functionality in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-2877	The extension system in Google Chrome before 22.0.1229.79 does not properly handle modal dialogs, which allows remote attackers to cause a denial of service (application crash) via unspecified vectors.
CVE-2012-2878	Use-after-free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to plug-in handling.
CVE-2012-2879	Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service (DOM topology corruption) via a crafted document.
CVE-2012-2880	Race condition in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the plug-in paint buffer.
CVE-2012-2881	Google Chrome before 22.0.1229.79 does not properly handle plug-ins, which allows remote attackers to cause a denial of service (DOM tree corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2012-2882	FFmpeg, as used in Google Chrome before 22.0.1229.79, does not properly handle OGG containers, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, related to a "wild pointer" issue.
CVE-2012-2883	Skia, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an out-of-bounds write operation, a different vulnerability than CVE-2012-2874.
CVE-2012-2884	Skia, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-2885	Double free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial

	of service or possibly have unspecified other impact via vectors related to application exit.
CVE-2012-2886	Cross-site scripting (XSS) vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to inject arbitrary web script or HTML via vectors related to the Google V8 bindings, aka "Universal XSS (UXSS)."
CVE-2012-2887	Use-after-free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving onclick events.
CVE-2012-2888	Use-after-free vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving SVG text references.
CVE-2012-2889	Cross-site scripting (XSS) vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to inject arbitrary web script or HTML via vectors involving frames, aka "Universal XSS (UXSS)."
CVE-2012-2890	Use-after-free vulnerability in the PDF functionality in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document.
CVE-2012-2891	The IPC implementation in Google Chrome before 22.0.1229.79 allows attackers to obtain potentially sensitive information about memory addresses via unspecified vectors.
CVE-2012-2892	Unspecified vulnerability in Google Chrome before 22.0.1229.79 allows remote attackers to bypass the pop-up blocker via unknown vectors.
CVE-2012-2893	Double free vulnerability in libxslt, as used in Google Chrome before 22.0.1229.79, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to XSL transforms.
CVE-2012-2894	Google Chrome before 22.0.1229.79 does not properly handle graphics-context data structures, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2012-2895	The PDF functionality in Google Chrome before 22.0.1229.79 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger out-of-bounds write operations.
CVE-2012-2900	Skia, as used in Google Chrome before 22.0.1229.92, does not properly render text, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via unknown vectors.

CVE-2012-2942	Buffer overflow in the trash buffer in the header capture functionality in HAProxy before 1.4.21, when global.tune.bufsize is set to a value greater than the default and header rewriting is enabled, allows remote attackers to cause a denial of service and possibly execute arbitrary code via unspecified vectors.
CVE-2012-3319	IBM Rational Business Developer 8.x before 8.0.1.4 allows remote attackers to obtain potentially sensitive information via a connection to a web service created with the Rational Business Developer product.
CVE-2012-3579	Symantec Messaging Gateway (SMG) before 10.0 has a default password for an unspecified account, which makes it easier for remote attackers to obtain privileged access via an SSH session.
CVE-2012-3580	Symantec Messaging Gateway (SMG) before 10.0 allows remote authenticated users to modify the web application by leveraging access to the management interface.
CVE-2012-3581	Symantec Messaging Gateway (SMG) before 10.0 allows remote attackers to obtain potentially sensitive information about component versions via unspecified vectors.
CVE-2012-3845	Buffer overflow in LAN Messenger 1.2.28 and earlier allows remote attackers to cause a denial of service (crash) via a long string in an initiation request.
CVE-2012-4010	Opera before 11.60 allows remote attackers to spoof the address bar via unspecified homograph characters, a different vulnerability than CVE-2010-2660.
CVE-2012-4142	Opera before 12.01 on Windows and UNIX, and before 11.66 and 12.x before 12.01 on Mac OS X, ignores some characters in HTML documents in unspecified circumstances, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via a crafted document.
CVE-2012-4143	Opera before 12.01 on Windows and UNIX, and before 11.66 and 12.x before 12.01 on Mac OS X, allows user-assisted remote attackers to trick users into downloading and executing arbitrary files via a small window for the download dialog, a different vulnerability than CVE-2012-1924.
CVE-2012-4144	Opera before 12.01 on Windows and UNIX, and before 11.66 and 12.x before 12.01 on Mac OS X, does not properly escape characters in DOM elements, which makes it easier for remote attackers to bypass cross-site scripting (XSS) protection mechanisms via a crafted HTML document.
CVE-2012-4145	Unspecified vulnerability in Opera before 12.01 on Windows and UNIX, and before 11.66 and 12.x before

	12.01 on Mac OS X, has unknown impact and attack vectors, related to a "low severity issue."
CVE-2012-4146	Opera before 12.01 allows remote attackers to cause a denial of service (application crash) via a crafted web site, as demonstrated by the Lenovo "Shop now" page.
CVE-2012-4163	Adobe Flash Player before 10.3.183.23 and 11.x before 11.4.402.265 on Windows and Mac OS X, before 10.3.183.23 and 11.x before 11.2.202.238 on Linux, before 11.1.111.16 on Android 2.x and 3.x, and before 11.1.115.17 on Android 4.x; Adobe AIR before 3.4.0.2540; and Adobe AIR SDK before 3.4.0.2540 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-4164 and CVE-2012-4165.
CVE-2012-4164	Adobe Flash Player before 10.3.183.23 and 11.x before 11.4.402.265 on Windows and Mac OS X, before 10.3.183.23 and 11.x before 11.2.202.238 on Linux, before 11.1.111.16 on Android 2.x and 3.x, and before 11.1.115.17 on Android 4.x; Adobe AIR before 3.4.0.2540; and Adobe AIR SDK before 3.4.0.2540 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-4163 and CVE-2012-4165.
CVE-2012-4165	Adobe Flash Player before 10.3.183.23 and 11.x before 11.4.402.265 on Windows and Mac OS X, before 10.3.183.23 and 11.x before 11.2.202.238 on Linux, before 11.1.111.16 on Android 2.x and 3.x, and before 11.1.115.17 on Android 4.x; Adobe AIR before 3.4.0.2540; and Adobe AIR SDK before 3.4.0.2540 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-4163 and CVE-2012-4164.
CVE-2012-4167	Integer overflow in Adobe Flash Player before 10.3.183.23 and 11.x before 11.4.402.265 on Windows and Mac OS X, before 10.3.183.23 and 11.x before 11.2.202.238 on Linux, before 11.1.111.16 on Android 2.x and 3.x, and before 11.1.115.17 on Android 4.x; Adobe AIR before 3.4.0.2540; and Adobe AIR SDK before 3.4.0.2540 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2012-4168	Adobe Flash Player before 10.3.183.23 and 11.x before 11.4.402.265 on Windows and Mac OS X, before 10.3.183.23 and 11.x before 11.2.202.238 on Linux, before 11.1.111.16 on Android 2.x and 3.x, and before 11.1.115.17 on Android 4.x; Adobe AIR before 3.4.0.2540; and Adobe AIR SDK before 3.4.0.2540 allow remote attackers to read content from a different domain via a crafted web site.

CVE-2012-4171	Adobe Flash Player before 10.3.183.23 and 11.x before 11.4.402.265 on Windows and Mac OS X, before 10.3.183.23 and 11.x before 11.2.202.238 on Linux, before 11.1.111.16 on Android 2.x and 3.x, and before 11.1.115.17 on Android 4.x; Adobe AIR before 3.4.0.2540; and Adobe AIR SDK before 3.4.0.2540 allow attackers to cause a denial of service (application crash) by leveraging a logic error during handling of Firefox dialogs.
CVE-2012-4347	Multiple directory traversal vulnerabilities in the management console in Symantec Messaging Gateway (SMG) 9.5.x allow remote authenticated users to read arbitrary files via a .. (dot dot) in the (1) logFile parameter in a logs action to brightmail/export or (2) localBackupFileSelection parameter in an APPLIANCE restoreSource action to brightmail/admin/restore/download.do.
CVE-2012-4607	Buffer overflow in nsrindexd in EMC NetWorker 7.5.x and 7.6.x before 7.6.5, and 8.x before 8.0.0.6, allows remote attackers to execute arbitrary code via crafted SunRPC data.
CVE-2012-4826	Stack-based buffer overflow in the SQL/PSM (aka SQL Persistent Stored Module) Stored Procedure (SP) infrastructure in IBM DB2 9.1, 9.5, 9.7 before FP7, 9.8, and 10.1 might allow remote authenticated users to execute arbitrary code by debugging a stored procedure.
CVE-2012-4842	Open redirect vulnerability in the web server in IBM Lotus Domino 8.5.x through 8.5.3 allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.
CVE-2012-4844	Cross-site scripting (XSS) vulnerability in the web server in IBM Lotus Domino 8.5.x through 8.5.3 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2012-4846	IBM Lotus Notes 8.5.x before 8.5.3 FP3 does not include the HTTPOnly flag in a Set-Cookie header for a web-application cookie, which makes it easier for remote attackers to obtain potentially sensitive information via script access to this cookie, aka SPRs JMAS7TRNLN and SRAO8U3Q68.
CVE-2012-4862	The Host Connect emulator in IBM Rational Developer for System z 7.1 through 8.5.1 does not properly store the SSL certificate password, which allows local users to obtain sensitive information via unspecified vectors.
CVE-2012-4956	Heap-based buffer overflow in NFRAgent.exe in Novell File Reporter 1.0.2 allows remote attackers to execute arbitrary code via a large number of VOL elements in an SRS record.

CVE-2012-4957	Absolute path traversal vulnerability in NFRAgent.exe in Novell File Reporter 1.0.2 allows remote attackers to read arbitrary files via a /FSF/CMD request with a full pathname in a PATH element of an SRS record.
CVE-2012-4958	Directory traversal vulnerability in NFRAgent.exe in Novell File Reporter 1.0.2 allows remote attackers to read arbitrary files via a 126 /FSF/CMD request with a .. (dot dot) in a FILE element of an FSFUI record.
CVE-2012-4959	Directory traversal vulnerability in NFRAgent.exe in Novell File Reporter 1.0.2 allows remote attackers to upload and execute files via a 130 /FSF/CMD request with a .. (dot dot) in a FILE element of an FSFUI record.
CVE-2012-5054	Integer overflow in the copyRawDataTo method in the Matrix3D class in Adobe Flash Player before 11.4.402.265 allows remote attackers to execute arbitrary code via malformed arguments.
CVE-2012-5108	Race condition in Google Chrome before 22.0.1229.92 allows remote attackers to execute arbitrary code via vectors related to audio devices.
CVE-2012-5109	The International Components for Unicode (ICU) functionality in Google Chrome before 22.0.1229.92 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to a regular expression.
CVE-2012-5110	The compositor in Google Chrome before 22.0.1229.92 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-5111	Google Chrome before 22.0.1229.92 does not monitor for crashes of Pepper plug-ins, which has unspecified impact and remote attack vectors.
CVE-2012-5112	Use-after-free vulnerability in the SVG implementation in WebKit, as used in Google Chrome before 22.0.1229.94, allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2012-5116	Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of SVG filters.
CVE-2012-5117	Google Chrome before 23.0.1271.64 does not properly restrict the loading of an SVG subresource in the context of an IMG element, which has unspecified impact and remote attack vectors.
CVE-2012-5119	Race condition in Pepper, as used in Google Chrome before 23.0.1271.64, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to buffers.
CVE-2012-5120	Google V8 before 3.13.7.5, as used in Google Chrome before 23.0.1271.64, on 64-bit Linux platforms allows remote attackers to cause a denial of service or

	possibly have unspecified other impact via crafted JavaScript code that triggers an out-of-bounds access to an array.
CVE-2012-5121	Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to video layout.
CVE-2012-5122	Google Chrome before 23.0.1271.64 does not properly perform a cast of an unspecified variable during handling of input, which allows remote attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2012-5123	Skia, as used in Google Chrome before 23.0.1271.64, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-5124	Google Chrome before 23.0.1271.64 does not properly handle textures, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2012-5125	Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of extension tabs.
CVE-2012-5126	Use-after-free vulnerability in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of plug-in placeholders.
CVE-2012-5127	Integer overflow in Google Chrome before 23.0.1271.64 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted WebP image.
CVE-2012-5128	Google V8 before 3.13.7.5, as used in Google Chrome before 23.0.1271.64, does not properly perform write operations, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-5130	Skia, as used in Google Chrome before 23.0.1271.91, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2012-5132	Google Chrome before 23.0.1271.91 allows remote attackers to cause a denial of service (application crash) via a response with chunked transfer coding.
CVE-2012-5133	Use-after-free vulnerability in Google Chrome before 23.0.1271.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to SVG filters.
CVE-2012-5134	Heap-based buffer underflow in the xmlParseAttValueComplex function in parser.c in libxml2 2.9.0 and earlier, as used in Google Chrome

	before 23.0.1271.91 and other products, allows remote attackers to cause a denial of service or possibly execute arbitrary code via crafted entities in an XML document.
CVE-2012-5135	Use-after-free vulnerability in Google Chrome before 23.0.1271.91 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to printing.
CVE-2012-5136	Google Chrome before 23.0.1271.91 does not properly perform a cast of an unspecified variable during handling of the INPUT element, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted HTML document.
CVE-2012-5137	Use-after-free vulnerability in Google Chrome before 23.0.1271.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the Media Source API.
CVE-2012-5138	Google Chrome before 23.0.1271.95 does not properly handle file paths, which has unspecified impact and attack vectors.
CVE-2012-5139	Use-after-free vulnerability in Google Chrome before 23.0.1271.97 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to visibility events.
CVE-2012-5140	Use-after-free vulnerability in Google Chrome before 23.0.1271.97 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the URL loader.
CVE-2012-5141	Google Chrome before 23.0.1271.97 does not properly restrict instantiation of the Chromoting client plug-in, which has unspecified impact and attack vectors.
CVE-2012-5142	Google Chrome before 23.0.1271.97 does not properly handle history navigation, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors.
CVE-2012-5143	Integer overflow in Google Chrome before 23.0.1271.97 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to PPAPI image buffers.
CVE-2012-5144	Google Chrome before 23.0.1271.97, and Libav 0.7.x before 0.7.7 and 0.8.x before 0.8.5, do not properly perform AAC decoding, which allows remote attackers to cause a denial of service (stack memory corruption) or possibly have unspecified other impact via vectors related to "an off-by-one overwrite when switching to LTP profile from MAIN."
CVE-2012-5145	Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial

	of service or possibly have unspecified other impact via vectors related to SVG layout.
CVE-2012-5146	Google Chrome before 24.0.1312.52 allows remote attackers to bypass the Same Origin Policy via a malformed URL.
CVE-2012-5147	Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOM handling.
CVE-2012-5148	The hyphenation functionality in Google Chrome before 24.0.1312.52 does not properly validate file names, which has unspecified impact and attack vectors.
CVE-2012-5149	Integer overflow in the audio IPC layer in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2012-5150	Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving seek operations on video data.
CVE-2012-5151	Integer overflow in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code in a PDF document.
CVE-2012-5152	Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors involving seek operations on video data.
CVE-2012-5153	Google V8 before 3.14.5.3, as used in Google Chrome before 24.0.1312.52, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers an out-of-bounds access to stack memory.
CVE-2012-5156	Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving PDF fields.
CVE-2012-5157	Google Chrome before 24.0.1312.52 does not properly handle image data in PDF documents, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted document.
CVE-2012-5248	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability

	than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5249	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5250	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5251	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5252	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5253	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability

	than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5254	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5255	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5256	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5257	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5258	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified

	vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5259	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5260	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5261	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5262	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5263	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified

	vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5264	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5265	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5266	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5267	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5268	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified

	vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5269	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5270	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5271	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5272	Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than other Flash Player memory corruption CVEs listed in APSB12-22.
CVE-2012-5274	Buffer overflow in Adobe Flash Player before 10.3.183.43 and 11.x before 11.5.502.110 on Windows and Mac OS X, before 10.3.183.43 and 11.x before 11.2.202.251 on Linux, before 11.1.111.24 on Android 2.x and 3.x, and before 11.1.115.27 on Android 4.x; Adobe AIR before 3.5.0.600; and Adobe AIR SDK before 3.5.0.600 allows attackers to execute arbitrary code via unspecified vectors, a different

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

	11.2.202.251 on Linux, before 11.1.111.24 on Android 2.x and 3.x, and before 11.1.115.27 on Android 4.x; Adobe AIR before 3.5.0.600; and Adobe AIR SDK before 3.5.0.600 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2012-5274, CVE-2012-5275, CVE-2012-5276, and CVE-2012-5277.
CVE-2012-5285	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5286	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5287	Buffer overflow in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than other Flash Player buffer overflow CVEs listed in APSB12-22.
CVE-2012-5376	The Inter-process Communication (IPC) implementation in Google Chrome before 22.0.1229.94 allows remote attackers to bypass intended sandbox restrictions and write to arbitrary files by leveraging access to a renderer process, a different vulnerability than CVE-2012-5112.
CVE-2012-5673	Unspecified vulnerability in Adobe Flash Player before 10.3.183.29 and 11.x before 11.4.402.287 on Windows and Mac OS X, before 10.3.183.29 and 11.x before 11.2.202.243 on Linux, before 11.1.111.19 on Android 2.x and 3.x, and before 11.1.115.20 on Android 4.x; Adobe AIR before 3.4.0.2710; and Adobe AIR SDK before 3.4.0.2710 has unknown impact and attack vectors.

CVE-2012-5675	Adobe ColdFusion 9.0 through 9.0.2, and 10, allows local users to bypass intended shared-hosting sandbox permissions via unspecified vectors.
CVE-2012-5676	Buffer overflow in Adobe Flash Player before 10.3.183.48 and 11.x before 11.5.502.135 on Windows, before 10.3.183.48 and 11.x before 11.5.502.136 on Mac OS X, before 10.3.183.48 and 11.x before 11.2.202.258 on Linux, before 11.1.111.29 on Android 2.x and 3.x, and before 11.1.115.34 on Android 4.x; Adobe AIR before 3.5.0.880 on Windows and before 3.5.0.890 on Mac OS X; and Adobe AIR SDK before 3.5.0.880 on Windows and before 3.5.0.890 on Mac OS X allows attackers to execute arbitrary code via unspecified vectors.
CVE-2012-5677	Integer overflow in Adobe Flash Player before 10.3.183.48 and 11.x before 11.5.502.135 on Windows, before 10.3.183.48 and 11.x before 11.5.502.136 on Mac OS X, before 10.3.183.48 and 11.x before 11.2.202.258 on Linux, before 11.1.111.29 on Android 2.x and 3.x, and before 11.1.115.34 on Android 4.x; Adobe AIR before 3.5.0.880 on Windows and before 3.5.0.890 on Mac OS X; and Adobe AIR SDK before 3.5.0.880 on Windows and before 3.5.0.890 on Mac OS X allows attackers to execute arbitrary code via unspecified vectors.
CVE-2012-5678	Adobe Flash Player before 10.3.183.48 and 11.x before 11.5.502.135 on Windows, before 10.3.183.48 and 11.x before 11.5.502.136 on Mac OS X, before 10.3.183.48 and 11.x before 11.2.202.258 on Linux, before 11.1.111.29 on Android 2.x and 3.x, and before 11.1.115.34 on Android 4.x; Adobe AIR before 3.5.0.880 on Windows and before 3.5.0.890 on Mac OS X; and Adobe AIR SDK before 3.5.0.880 on Windows and before 3.5.0.890 on Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2012-5851	html/parser/XSSAuditor.cpp in WebCore in WebKit, as used in Google Chrome through 22 and Safari 5.1.7, does not consider all possible output contexts of reflected data, which makes it easier for remote attackers to bypass a cross-site scripting (XSS) protection mechanism via a crafted string, aka rdar problem 12019108.
CVE-2012-5956	Multiple cross-site scripting (XSS) vulnerabilities in ManageEngine AssetExplorer 5.6 before service pack 5614 allow remote attackers to inject arbitrary web script or HTML via fields in XML asset data to discoveryServlet/WsDiscoveryServlet, as demonstrated by the DocRoot/Computer_Information/output element.
CVE-2012-6460	Opera before 11.67 and 12.x before 12.02 allows remote attackers to cause truncation of a dialog, and

	possibly trigger downloading and execution of arbitrary programs, via a crafted web site.
CVE-2012-6461	The X.509 certificate-validation functionality in the https implementation in Opera before 12.10 allows remote attackers to trigger a false indication of successful revocation-status checking by causing a failure of a single checking service.
CVE-2012-6462	Opera before 12.10 does not properly implement the Cross-Origin Resource Sharing (CORS) specification, which allows remote attackers to bypass intended page-content restrictions via a crafted request.
CVE-2012-6463	Cross-site scripting (XSS) vulnerability in Opera before 12.10 allows remote attackers to inject arbitrary web script or HTML via vectors involving an unspecified sequence of loading of documents and loading of data: URLs.
CVE-2012-6464	Cross-site scripting (XSS) vulnerability in Opera before 12.10 allows remote attackers to inject arbitrary web script or HTML via crafted JavaScript code that overrides methods of unspecified native objects in documents that have different origins.
CVE-2012-6465	Opera before 12.10 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via a malformed SVG image.
CVE-2012-6466	Opera before 12.10 does not properly handle incorrect size data in a WebP image, which allows remote attackers to obtain potentially sensitive information from process memory by using a crafted image as the fill pattern for a canvas.
CVE-2012-6467	Opera before 12.10 follows Internet shortcuts that are referenced by a (1) IMG element or (2) other inline element, which makes it easier for remote attackers to conduct phishing attacks via a crafted web site, as exploited in the wild in November 2012.
CVE-2012-6468	Heap-based buffer overflow in Opera before 12.11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a long HTTP response.
CVE-2012-6469	Opera before 12.11 allows remote attackers to determine the existence of arbitrary local files via vectors involving web script in an error page.
CVE-2012-6470	Opera before 12.12 does not properly allocate memory for GIF images, which allows remote attackers to execute arbitrary code or cause a denial of service (memory overwrite) via a malformed image.
CVE-2012-6471	Opera before 12.12 allows remote attackers to spoof the address field via a high rate of HTTP requests.
CVE-2012-6472	Opera before 12.12 on UNIX uses weak permissions for the profile directory, which allows local users to

	obtain sensitive information by reading a (1) cache file, (2) password file, or (3) configuration file, or (4) possibly gain privileges by modifying or overwriting a configuration file.
CVE-2012-6702	Expat, when used in a parser that has not called XML_SetHashSalt or passed it a seed of 0, makes it easier for context-dependent attackers to defeat cryptographic protection mechanisms via vectors involving use of the srand function.
CVE-2013-0471	The traditional scheduler in the client in IBM Tivoli Storage Manager (TSM) before 6.2.5.0, 6.3 before 6.3.1.0, and 6.4 before 6.4.0.1, when Prompted mode is enabled, allows remote attackers to cause a denial of service (scheduling outage) via unspecified vectors.
CVE-2013-0472	The Web GUI in the client in IBM Tivoli Storage Manager (TSM) 6.3 before 6.3.1.0 and 6.4 before 6.4.0.1 allows man-in-the-middle attackers to obtain unspecified client access, and consequently obtain unspecified server access, via unknown vectors.
CVE-2013-0504	Buffer overflow in the broker service in Adobe Flash Player before 10.3.183.67 and 11.x before 11.6.602.171 on Windows and Mac OS X, and before 10.3.183.67 and 11.x before 11.2.202.273 on Linux, allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-0601	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-1530, CVE-2013-0605, CVE-2013-0616, CVE-2013-0619, CVE-2013-0620, and CVE-2013-0623.
CVE-2013-0602	Use-after-free vulnerability in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-0603	Heap-based buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0604.
CVE-2013-0604	Heap-based buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0603.
CVE-2013-0605	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different

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

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

CVE-2013-0622	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2013-0624.
CVE-2013-0623	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2012-1530, CVE-2013-0601, CVE-2013-0605, CVE-2013-0616, CVE-2013-0619, and CVE-2013-0620.
CVE-2013-0624	Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2013-0622.
CVE-2013-0625	Adobe ColdFusion 9.0, 9.0.1, and 9.0.2, when a password is not configured, allows remote attackers to bypass authentication and possibly execute arbitrary code via unspecified vectors, as exploited in the wild in January 2013.
CVE-2013-0626	Stack-based buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0610.
CVE-2013-0627	Unspecified vulnerability in Adobe Reader and Acrobat 9.x before 9.5.3, 10.x before 10.1.5, and 11.x before 11.0.1 allows local users to gain privileges via unknown vectors.
CVE-2013-0629	Adobe ColdFusion 9.0, 9.0.1, 9.0.2, and 10, when a password is not configured, allows attackers to access restricted directories via unspecified vectors, as exploited in the wild in January 2013.
CVE-2013-0630	Buffer overflow in Adobe Flash Player before 10.3.183.50 and 11.x before 11.5.502.146 on Windows and Mac OS X, before 10.3.183.50 and 11.x before 11.2.202.261 on Linux, before 11.1.111.31 on Android 2.x and 3.x, and before 11.1.115.36 on Android 4.x; Adobe AIR before 3.5.0.1060; and Adobe AIR SDK before 3.5.0.1060 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-0631	Adobe ColdFusion 9.0, 9.0.1, and 9.0.2 allows attackers to obtain sensitive information via unspecified vectors, as exploited in the wild in January 2013.
CVE-2013-0632	administrator.cfc in Adobe ColdFusion 9.0, 9.0.1, 9.0.2, and 10 allows remote attackers to bypass authentication and possibly execute arbitrary code by logging in to the RDS component using the default empty password and leveraging this session to access

	the administrative web interface, as exploited in the wild in January 2013.
CVE-2013-0633	Buffer overflow in Adobe Flash Player before 10.3.183.51 and 11.x before 11.5.502.149 on Windows and Mac OS X, before 10.3.183.51 and 11.x before 11.2.202.262 on Linux, before 11.1.111.32 on Android 2.x and 3.x, and before 11.1.115.37 on Android 4.x allows remote attackers to execute arbitrary code via crafted SWF content, as exploited in the wild in February 2013.
CVE-2013-0634	Adobe Flash Player before 10.3.183.51 and 11.x before 11.5.502.149 on Windows and Mac OS X, before 10.3.183.51 and 11.x before 11.2.202.262 on Linux, before 11.1.111.32 on Android 2.x and 3.x, and before 11.1.115.37 on Android 4.x allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted SWF content, as exploited in the wild in February 2013.
CVE-2013-0637	Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allow attackers to obtain sensitive information via unspecified vectors.
CVE-2013-0638	Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-0647.
CVE-2013-0639	Integer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-0640	Adobe Reader and Acrobat 9.x before 9.5.4, 10.x before 10.1.6, and 11.x before 11.0.02 allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted PDF document, as exploited in the wild in February 2013.

CVE-2013-0641	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.4, 10.x before 10.1.6, and 11.x before 11.0.02 allows remote attackers to execute arbitrary code via a crafted PDF document, as exploited in the wild in February 2013.
CVE-2013-0642	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0645, CVE-2013-1365, CVE-2013-1366, CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, CVE-2013-1372, and CVE-2013-1373.
CVE-2013-0643	The Firefox sandbox in Adobe Flash Player before 10.3.183.67 and 11.x before 11.6.602.171 on Windows and Mac OS X, and before 10.3.183.67 and 11.x before 11.2.202.273 on Linux, does not properly restrict privileges, which makes it easier for remote attackers to execute arbitrary code via crafted SWF content, as exploited in the wild in February 2013.
CVE-2013-0644	Use-after-free vulnerability in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0649 and CVE-2013-1374.
CVE-2013-0645	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0642, CVE-2013-1365, CVE-2013-1366, CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, CVE-2013-1372, and CVE-2013-1373.
CVE-2013-0646	Integer overflow in Adobe Flash Player before 10.3.183.68 and 11.x before 11.6.602.180 on Windows and Mac OS X, before 10.3.183.68 and 11.x before

	11.2.202.275 on Linux, before 11.1.111.44 on Android 2.x and 3.x, and before 11.1.115.48 on Android 4.x; Adobe AIR before 3.6.0.6090; Adobe AIR SDK before 3.6.0.6090; and Adobe AIR SDK & Compiler before 3.6.0.6090 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-0647	Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-0638.
CVE-2013-0648	Unspecified vulnerability in the ExternalInterface ActionScript functionality in Adobe Flash Player before 10.3.183.67 and 11.x before 11.6.602.171 on Windows and Mac OS X, and before 10.3.183.67 and 11.x before 11.2.202.273 on Linux, allows remote attackers to execute arbitrary code via crafted SWF content, as exploited in the wild in February 2013.
CVE-2013-0649	Use-after-free vulnerability in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0644 and CVE-2013-1374.
CVE-2013-0650	Use-after-free vulnerability in Adobe Flash Player before 10.3.183.68 and 11.x before 11.6.602.180 on Windows and Mac OS X, before 10.3.183.68 and 11.x before 11.2.202.275 on Linux, before 11.1.111.44 on Android 2.x and 3.x, and before 11.1.115.48 on Android 4.x; Adobe AIR before 3.6.0.6090; Adobe AIR SDK before 3.6.0.6090; and Adobe AIR SDK & Compiler before 3.6.0.6090 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-0828	The PDF functionality in Google Chrome before 24.0.1312.52 does not properly perform a cast of an unspecified variable during processing of the root of the structure tree, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted document.
CVE-2013-0829	Google Chrome before 24.0.1312.52 does not properly maintain database metadata, which allows remote

	attackers to bypass intended file-access restrictions via unspecified vectors.
CVE-2013-0831	Directory traversal vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to have an unspecified impact by leveraging access to an extension process.
CVE-2013-0832	Use-after-free vulnerability in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to printing.
CVE-2013-0833	Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to printing.
CVE-2013-0834	Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors involving glyphs.
CVE-2013-0835	Unspecified vulnerability in the Geolocation implementation in Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service (application crash) via unknown vectors.
CVE-2013-0836	Google V8 before 3.14.5.3, as used in Google Chrome before 24.0.1312.52, does not properly implement garbage collection, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2013-0837	Google Chrome before 24.0.1312.52 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of extension tabs.
CVE-2013-0838	Google Chrome before 24.0.1312.52 on Linux uses weak permissions for shared memory segments, which has unspecified impact and attack vectors.
CVE-2013-0839	Use-after-free vulnerability in Google Chrome before 24.0.1312.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of fonts in CANVAS elements.
CVE-2013-0840	Google Chrome before 24.0.1312.56 does not validate URLs during the opening of new windows, which has unspecified impact and remote attack vectors.
CVE-2013-0841	Array index error in the content-blocking functionality in Google Chrome before 24.0.1312.56 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0842	Google Chrome before 24.0.1312.56 does not properly handle %00 characters in pathnames, which has unspecified impact and attack vectors.

CVE-2013-0879	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly implement web audio nodes, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-0880	Use-after-free vulnerability in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to databases.
CVE-2013-0881	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (incorrect read operation) via crafted data in the Matroska container format.
CVE-2013-0882	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (incorrect memory access) or possibly have unspecified other impact via a large number of SVG parameters.
CVE-2013-0883	Skia, as used in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (incorrect read operation) via unspecified vectors.
CVE-2013-0884	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly load Native Client (aka NaCl) code, which has unspecified impact and attack vectors.
CVE-2013-0885	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly restrict API privileges during interaction with the Chrome Web Store, which has unspecified impact and attack vectors.
CVE-2013-0887	The developer-tools process in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly restrict privileges during interaction with a connected server, which has unspecified impact and attack vectors.
CVE-2013-0888	Skia, as used in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to a "user gesture check for dangerous file downloads."
CVE-2013-0889	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly enforce a user gesture requirement before proceeding with a file download, which might make it

	easier for remote attackers to execute arbitrary code via a crafted file.
CVE-2013-0890	Multiple unspecified vulnerabilities in the IPC layer in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allow remote attackers to cause a denial of service (memory corruption) or possibly have other impact via unknown vectors.
CVE-2013-0891	Integer overflow in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a blob.
CVE-2013-0892	Multiple unspecified vulnerabilities in the IPC layer in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allow remote attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-0893	Race condition in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to media.
CVE-2013-0894	Buffer overflow in the vorbis_parse_setup_hdr_floors function in the Vorbis decoder in vorbisdec.c in libavcodec in FFmpeg through 1.1.3, as used in Google Chrome before 25.0.1364.97 on Windows and Linux and before 25.0.1364.99 on Mac OS X and other products, allows remote attackers to cause a denial of service (divide-by-zero error or out-of-bounds array access) or possibly have unspecified other impact via vectors involving a zero value for a bark map size.
CVE-2013-0895	Google Chrome before 25.0.1364.97 on Linux, and before 25.0.1364.99 on Mac OS X, does not properly handle pathnames during copy operations, which might make it easier for remote attackers to execute arbitrary programs via unspecified vectors.
CVE-2013-0896	Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, does not properly manage memory during message handling for plug-ins, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0897	Off-by-one error in the PDF functionality in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service via a crafted document.
CVE-2013-0898	Use-after-free vulnerability in Google Chrome before 25.0.1364.97 on Windows and Linux, and before

	25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a URL.
CVE-2013-0899	Integer overflow in the padding implementation in the opus_packet_parse_impl function in src/opus_decoder.c in Opus before 1.0.2, as used in Google Chrome before 25.0.1364.97 on Windows and Linux and before 25.0.1364.99 on Mac OS X and other products, allows remote attackers to cause a denial of service (out-of-bounds read) via a long packet.
CVE-2013-0900	Race condition in the International Components for Unicode (ICU) functionality in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0902	Use-after-free vulnerability in the frame-loader implementation in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0903	Use-after-free vulnerability in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of browser navigation.
CVE-2013-0904	The Web Audio implementation in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-0905	Use-after-free vulnerability in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving an SVG animation.
CVE-2013-0906	The IndexedDB implementation in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-0907	Race condition in Google Chrome before 25.0.1364.152 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of media threads.
CVE-2013-0908	Google Chrome before 25.0.1364.152 does not properly manage bindings of extension processes, which has unspecified impact and attack vectors.
CVE-2013-0909	The XSS Auditor in Google Chrome before 25.0.1364.152 allows remote attackers to obtain sensitive HTTP Referer information via unspecified vectors.

CVE-2013-0910	Google Chrome before 25.0.1364.152 does not properly manage the interaction between the browser process and renderer processes during authorization of the loading of a plug-in, which makes it easier for remote attackers to bypass intended access restrictions via vectors involving a blocked plug-in.
CVE-2013-0911	Directory traversal vulnerability in Google Chrome before 25.0.1364.152 allows remote attackers to have an unspecified impact via vectors related to databases.
CVE-2013-0912	WebKit in Google Chrome before 25.0.1364.160 allows remote attackers to execute arbitrary code via vectors that leverage "type confusion."
CVE-2013-0916	Use-after-free vulnerability in the Web Audio implementation in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0917	The URL loader in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2013-0918	Google Chrome before 26.0.1410.43 does not prevent navigation to developer tools in response to a drag-and-drop operation, which allows user-assisted remote attackers to have an unspecified impact via a crafted web site.
CVE-2013-0919	Use-after-free vulnerability in Google Chrome before 26.0.1410.43 on Linux allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging the presence of an extension that creates a pop-up window.
CVE-2013-0920	Use-after-free vulnerability in the extension bookmarks API in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-0921	The Isolated Sites feature in Google Chrome before 26.0.1410.43 does not properly enforce the use of separate processes, which makes it easier for remote attackers to bypass intended access restrictions via a crafted web site.
CVE-2013-0922	Google Chrome before 26.0.1410.43 does not properly restrict brute-force access attempts against web sites that require HTTP Basic Authentication, which has unspecified impact and attack vectors.
CVE-2013-0923	The USB Apps API in Google Chrome before 26.0.1410.43 allows remote attackers to cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-0924	The extension functionality in Google Chrome before 26.0.1410.43 does not verify that use of the

	permissions API is consistent with file permissions, which has unspecified impact and attack vectors.
CVE-2013-0925	Google Chrome before 26.0.1410.43 does not ensure that an extension has the tabs (aka APIPermission::kTab) permission before providing a URL to this extension, which has unspecified impact and remote attack vectors.
CVE-2013-0926	Google Chrome before 26.0.1410.43 does not properly handle active content in an EMBED element during a copy-and-paste operation, which allows user-assisted remote attackers to have an unspecified impact via a crafted web site.
CVE-2013-0940	The nsrpush process in the client in EMC NetWorker before 7.6.5.3 and 8.x before 8.0.1.4 sets weak permissions for unspecified files, which allows local users to gain privileges via unknown vectors.
CVE-2013-1365	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0642, CVE-2013-0645, CVE-2013-1366, CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, CVE-2013-1372, and CVE-2013-1373.
CVE-2013-1366	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0642, CVE-2013-0645, CVE-2013-1365, CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, CVE-2013-1372, and CVE-2013-1373.
CVE-2013-1367	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different

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

	attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-1372	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0642, CVE-2013-0645, CVE-2013-1365, CVE-2013-1366, CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, and CVE-2013-1373.
CVE-2013-1373	Buffer overflow in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0642, CVE-2013-0645, CVE-2013-1365, CVE-2013-1366, CVE-2013-1367, CVE-2013-1368, CVE-2013-1369, CVE-2013-1370, and CVE-2013-1372.
CVE-2013-1374	Use-after-free vulnerability in Adobe Flash Player before 10.3.183.63 and 11.x before 11.6.602.168 on Windows, before 10.3.183.61 and 11.x before 11.6.602.167 on Mac OS X, before 10.3.183.61 and 11.x before 11.2.202.270 on Linux, before 11.1.111.43 on Android 2.x and 3.x, and before 11.1.115.47 on Android 4.x; Adobe AIR before 3.6.0.597; and Adobe AIR SDK before 3.6.0.599 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-0644 and CVE-2013-0649.
CVE-2013-1375	Heap-based buffer overflow in Adobe Flash Player before 10.3.183.68 and 11.x before 11.6.602.180 on Windows and Mac OS X, before 10.3.183.68 and 11.x before 11.2.202.275 on Linux, before 11.1.111.44 on Android 2.x and 3.x, and before 11.1.115.48 on Android 4.x; Adobe AIR before 3.6.0.6090; Adobe AIR SDK before 3.6.0.6090; and Adobe AIR SDK & Compiler before 3.6.0.6090 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-1378	Adobe Flash Player before 10.3.183.75 and 11.x before 11.7.700.169 on Windows and Mac OS X, before 10.3.183.75 and 11.x before 11.2.202.280 on Linux, before 11.1.111.50 on Android 2.x and 3.x,

	and before 11.1.115.54 on Android 4.x; Adobe AIR before 3.7.0.1530; and Adobe AIR SDK & Compiler before 3.7.0.1530 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-1380.
CVE-2013-1379	Adobe Flash Player before 10.3.183.75 and 11.x before 11.7.700.169 on Windows and Mac OS X, before 10.3.183.75 and 11.x before 11.2.202.280 on Linux, before 11.1.111.50 on Android 2.x and 3.x, and before 11.1.115.54 on Android 4.x; Adobe AIR before 3.7.0.1530; and Adobe AIR SDK & Compiler before 3.7.0.1530 do not properly initialize pointer arrays, which allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-1380	Adobe Flash Player before 10.3.183.75 and 11.x before 11.7.700.169 on Windows and Mac OS X, before 10.3.183.75 and 11.x before 11.2.202.280 on Linux, before 11.1.111.50 on Android 2.x and 3.x, and before 11.1.115.54 on Android 4.x; Adobe AIR before 3.7.0.1530; and Adobe AIR SDK & Compiler before 3.7.0.1530 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-1378.
CVE-2013-1618	The TLS implementation in Opera before 12.13 does not properly consider timing side-channel attacks on a MAC check operation during the processing of malformed CBC padding, which allows remote attackers to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data for crafted packets, a related issue to CVE-2013-0169.
CVE-2013-1637	Opera before 12.13 allows remote attackers to execute arbitrary code via vectors involving DOM events.
CVE-2013-1638	Opera before 12.13 allows remote attackers to execute arbitrary code via crafted clipPaths in an SVG document.
CVE-2013-1639	Opera before 12.13 does not send CORS preflight requests in all required cases, which allows remote attackers to bypass a CSRF protection mechanism via a crafted web site that triggers a CORS request.
CVE-2013-2268	Unspecified vulnerability in the MathML implementation in WebKit in Google Chrome before 25.0.1364.97 on Windows and Linux, and before 25.0.1364.99 on Mac OS X, has unknown impact and remote attack vectors, related to a "high severity security issue."
CVE-2013-2503	Privoxy before 3.0.21 does not properly handle Proxy-Authenticate and Proxy-Authorization headers in the

	client-server data stream, which makes it easier for remote HTTP servers to spoof the intended proxy service via a 407 (aka Proxy Authentication Required) HTTP status code.
CVE-2013-2549	Unspecified vulnerability in Adobe Reader 11.0.02 allows remote attackers to execute arbitrary code via vectors related to a "break into the sandbox," as demonstrated by George Hotz during a Pwn2Own competition at CanSecWest 2013.
CVE-2013-2550	Unspecified vulnerability in Adobe Reader 11.0.02 allows attackers to bypass the sandbox protection mechanism via unknown vectors, as demonstrated by George Hotz during a Pwn2Own competition at CanSecWest 2013.
CVE-2013-2555	Integer overflow in Adobe Flash Player before 10.3.183.75 and 11.x before 11.7.700.169 on Windows and Mac OS X, before 10.3.183.75 and 11.x before 11.2.202.280 on Linux, before 11.1.111.50 on Android 2.x and 3.x, and before 11.1.115.54 on Android 4.x; Adobe AIR before 3.7.0.1530; and Adobe AIR SDK & Compiler before 3.7.0.1530 allows remote attackers to execute arbitrary code via unspecified vectors, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2013.
CVE-2013-2632	Google V8 before 3.17.13, as used in Google Chrome before 27.0.1444.3, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code, as demonstrated by the Bejeweled game.
CVE-2013-2718	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2719	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.

CVE-2013-2720	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2721	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2722	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2723	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2724	Stack-based buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-2725	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of

	service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2726	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2727	Integer overflow in Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-2729.
CVE-2013-2728	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-3324, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.
CVE-2013-2729	Integer overflow in Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-2727.
CVE-2013-2730	Buffer overflow in Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2013-2733.
CVE-2013-2731	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of

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

	CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, CVE-2013-3340, and CVE-2013-3341.
CVE-2013-2737	A JavaScript API in Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allows attackers to obtain sensitive information via unspecified vectors.
CVE-2013-2741	importbuddy.php in the BackupBuddy plugin 1.3.4, 2.1.4, 2.2.25, 2.2.28, and 2.2.4 for WordPress does not require that authentication be enabled, which allows remote attackers to obtain sensitive information, or overwrite or delete files, via vectors involving a (1) direct request, (2) step=1 request, (3) step=2 or step=3 request, or (4) step=7 request.
CVE-2013-2766	Cross-site scripting (XSS) vulnerability in Splunk Web in Splunk 4.3.0 through 4.3.5 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2013-2836	Multiple unspecified vulnerabilities in Google Chrome before 27.0.1453.93 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2837	Use-after-free vulnerability in the SVG implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2838	Google V8, as used in Google Chrome before 27.0.1453.93, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2013-2839	Google Chrome before 27.0.1453.93 does not properly perform a cast of an unspecified variable during handling of clipboard data, which allows remote attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2840	Use-after-free vulnerability in the media loader in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2013-2846.
CVE-2013-2841	Use-after-free vulnerability in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of Pepper resources.
CVE-2013-2842	Use-after-free vulnerability in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial

	of service or possibly have unspecified other impact via vectors related to the handling of widgets.
CVE-2013-2843	Use-after-free vulnerability in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of speech data.
CVE-2013-2844	Use-after-free vulnerability in the Cascading Style Sheets (CSS) implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to style resolution.
CVE-2013-2845	The Web Audio implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2846	Use-after-free vulnerability in the media loader in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2013-2840.
CVE-2013-2847	Race condition in the workers implementation in Google Chrome before 27.0.1453.93 allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2848	The XSS Auditor in Google Chrome before 27.0.1453.93 might allow remote attackers to obtain sensitive information via unspecified vectors.
CVE-2013-2849	Multiple cross-site scripting (XSS) vulnerabilities in Google Chrome before 27.0.1453.93 allow user-assisted remote attackers to inject arbitrary web script or HTML via vectors involving a (1) drag-and-drop or (2) copy-and-paste operation.
CVE-2013-2853	The HTTPS implementation in Google Chrome before 28.0.1500.71 does not ensure that headers are terminated by \r\n\r\n (carriage return, newline, carriage return, newline), which allows man-in-the-middle attackers to have an unspecified impact via vectors that trigger header truncation.
CVE-2013-2855	The Developer Tools API in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2856	Use-after-free vulnerability in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of input.
CVE-2013-2857	Use-after-free vulnerability in Google Chrome before 27.0.1453.110 allows remote attackers to cause a

	denial of service or possibly have unspecified other impact via vectors related to the handling of images.
CVE-2013-2858	Use-after-free vulnerability in the HTML5 Audio implementation in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2859	Google Chrome before 27.0.1453.110 allows remote attackers to bypass the Same Origin Policy and trigger namespace pollution via unspecified vectors.
CVE-2013-2860	Use-after-free vulnerability in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving access to a database API by a worker process.
CVE-2013-2861	Use-after-free vulnerability in the SVG implementation in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2862	Skia, as used in Google Chrome before 27.0.1453.110, does not properly handle GPU acceleration, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2863	Google Chrome before 27.0.1453.110 does not properly handle SSL sockets, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-2864	The PDF functionality in Google Chrome before 27.0.1453.110 allows remote attackers to cause a denial of service (invalid free operation) or possibly have unspecified other impact via unknown vectors.
CVE-2013-2865	Multiple unspecified vulnerabilities in Google Chrome before 27.0.1453.110 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2867	Google Chrome before 28.0.1500.71 does not properly prevent pop-under windows, which allows remote attackers to have an unspecified impact via a crafted web site.
CVE-2013-2868	common/extensions/sync_helper.cc in Google Chrome before 28.0.1500.71 proceeds with sync operations for NPAPI extensions without checking for a certain plugin permission setting, which might allow remote attackers to trigger unwanted extension changes via unspecified vectors.
CVE-2013-2869	Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted JPEG2000 image.

CVE-2013-2870	Use-after-free vulnerability in Google Chrome before 28.0.1500.71 allows remote servers to execute arbitrary code via crafted response traffic after a URL request.
CVE-2013-2871	Use-after-free vulnerability in Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the handling of input.
CVE-2013-2873	Use-after-free vulnerability in Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a 404 HTTP status code during the loading of resources.
CVE-2013-2875	core/rendering/svg/SVGInlineTextBox.cpp in the SVG implementation in Blink, as used in Google Chrome before 28.0.1500.71, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2013-2876	browser/extensions/api/tabs/tabs_api.cc in Google Chrome before 28.0.1500.71 does not properly enforce restrictions on the capture of screenshots by extensions, which allows remote attackers to obtain sensitive information about the content of a previous page via vectors involving an interstitial page.
CVE-2013-2877	parser.c in libxml2 before 2.9.0, as used in Google Chrome before 28.0.1500.71 and other products, allows remote attackers to cause a denial of service (out-of-bounds read) via a document that ends abruptly, related to the lack of certain checks for the XML_PARSER_EOF state.
CVE-2013-2878	Google Chrome before 28.0.1500.71 allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the handling of text.
CVE-2013-2879	Google Chrome before 28.0.1500.71 does not properly determine the circumstances in which a renderer process can be considered a trusted process for sign-in and subsequent sync operations, which makes it easier for remote attackers to conduct phishing attacks via a crafted web site.
CVE-2013-2880	Multiple unspecified vulnerabilities in Google Chrome before 28.0.1500.71 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2881	Google Chrome before 28.0.1500.95 does not properly handle frames, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2013-2882	Google V8, as used in Google Chrome before 28.0.1500.95, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."

CVE-2013-2883	Use-after-free vulnerability in Google Chrome before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to deleting the registration of a MutationObserver object.
CVE-2013-2884	Use-after-free vulnerability in the DOM implementation in Google Chrome before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to improper tracking of which document owns an Attr object.
CVE-2013-2885	Use-after-free vulnerability in Google Chrome before 28.0.1500.95 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to not properly considering focus during the processing of JavaScript events in the presence of a multiple-fields input type.
CVE-2013-2886	Multiple unspecified vulnerabilities in Google Chrome before 28.0.1500.95 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2887	Multiple unspecified vulnerabilities in Google Chrome before 29.0.1547.57 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2900	The FilePath::ReferencesParent function in files/file_path.cc in Google Chrome before 29.0.1547.57 on Windows does not properly handle pathname components composed entirely of . (dot) and whitespace characters, which allows remote attackers to conduct directory traversal attacks via a crafted directory name.
CVE-2013-2901	Multiple integer overflows in (1) libGLESv2/renderer/Renderer9.cpp and (2) libGLESv2/renderer/Renderer11.cpp in Almost Native Graphics Layer Engine (ANGLE), as used in Google Chrome before 29.0.1547.57, allow remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2902	Use-after-free vulnerability in the XSLT ProcessingInstruction implementation in Blink, as used in Google Chrome before 29.0.1547.57, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to an applyXSLTransform call involving (1) an HTML document or (2) an xsl:processing-instruction element that is still in the process of loading.
CVE-2013-2903	Use-after-free vulnerability in the HTMLMediaElement::didMoveToNewDocument function in core/html/HTMLMediaElement.cpp in Blink, as used in Google Chrome before 29.0.1547.57,

	allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving moving a (1) AUDIO or (2) VIDEO element between documents.
CVE-2013-2904	Use-after-free vulnerability in the Document::finishedParsing function in core/dom/Document.cpp in Blink, as used in Google Chrome before 29.0.1547.57, allows remote attackers to cause a denial of service or possibly have unspecified other impact via an onload event that changes an IFRAME element so that its src attribute is no longer an XML document, leading to unintended garbage collection of this document.
CVE-2013-2905	The SharedMemory::Create function in memory/shared_memory_posix.cc in Google Chrome before 29.0.1547.57 uses weak permissions under /dev/shm/, which allows attackers to obtain sensitive information via direct access to a POSIX shared-memory file.
CVE-2013-2906	Multiple race conditions in the Web Audio implementation in Blink, as used in Google Chrome before 30.0.1599.66, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to threading in core/html/HTMLMediaElement.cpp, core/platform/audio/AudioDSPKernelProcessor.cpp, core/platform/audio/HRTFElevation.cpp, and modules/webaudio/ConvolverNode.cpp.
CVE-2013-2907	The Window.prototype object implementation in Google Chrome before 30.0.1599.66 allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2013-2908	Google Chrome before 30.0.1599.66 uses incorrect function calls to determine the values of NavigationEntry objects, which allows remote attackers to spoof the address bar via vectors involving a response with a 204 (aka No Content) status code.
CVE-2013-2909	Use-after-free vulnerability in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to inline-block rendering for bidirectional Unicode text in an element isolated from its siblings.
CVE-2013-2910	Use-after-free vulnerability in modules/webaudio/AudioScheduledSourceNode.cpp in the Web Audio implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2911	Use-after-free vulnerability in the XSLStyleSheet::compileStyleSheet function in core/

	xml/XSLStyleSheetLibxslt.cpp in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of post-failure recompilation in unspecified libxslt versions.
CVE-2013-2912	Use-after-free vulnerability in the PepperInProcessRouter::SendToHost function in content/renderer/pepper/pepper_in_process_router.cc in the Pepper Plug-in API (PPAPI) in Google Chrome before 30.0.1599.66 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving a resource-destruction message.
CVE-2013-2913	Use-after-free vulnerability in the XMLDocumentParser::append function in core/xml/parser/XMLDocumentParser.cpp in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors involving an XML document.
CVE-2013-2915	Google Chrome before 30.0.1599.66 preserves pending NavigationEntry objects in certain invalid circumstances, which allows remote attackers to spoof the address bar via a URL with a malformed scheme, as demonstrated by a nonexistent:12121 URL.
CVE-2013-2916	Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to spoof the address bar via vectors involving a response with a 204 (aka No Content) status code, in conjunction with a delay in notifying the user of an attempted spoof.
CVE-2013-2917	The ReverbConvolverStage::ReverbConvolverStage function in core/platform/audio/ReverbConvolverStage.cpp in the Web Audio implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service (out-of-bounds read) via vectors related to the impulseResponse array.
CVE-2013-2918	Use-after-free vulnerability in the RenderBlock::collapseAnonymousBlockChild function in core/rendering/RenderBlock.cpp in the DOM implementation in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect handling of parent-child relationships for anonymous blocks.
CVE-2013-2919	Google V8, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.

CVE-2013-2920	The DoResolveRelativeHost function in url/url_canon_relative.cc in Google Chrome before 30.0.1599.66 allows remote attackers to cause a denial of service (out-of-bounds read) via a relative URL containing a hostname, as demonstrated by a protocol-relative URL beginning with a //www.google.com/ substring.
CVE-2013-2921	Double free vulnerability in the ResourceFetcher::didLoadResource function in core/fetch/ResourceFetcher.cpp in the resource loader in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering certain callback processing during the reporting of a resource entry.
CVE-2013-2922	Use-after-free vulnerability in core/html/HTMLTemplateElement.cpp in Blink, as used in Google Chrome before 30.0.1599.66, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that operates on a TEMPLATE element.
CVE-2013-2923	Multiple unspecified vulnerabilities in Google Chrome before 30.0.1599.66 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2924	Use-after-free vulnerability in International Components for Unicode (ICU), as used in Google Chrome before 30.0.1599.66 and other products, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2013-2925	Use-after-free vulnerability in core/xml/XMLHttpRequest.cpp in Blink, as used in Google Chrome before 30.0.1599.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger multiple conflicting uses of the same XMLHttpRequest object.
CVE-2013-2926	Use-after-free vulnerability in the IndentOutdentCommand::tryIndentingAsListItem function in core/editing/IndentOutdentCommand.cpp in Blink, as used in Google Chrome before 30.0.1599.101, allows user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to list elements.
CVE-2013-2927	Use-after-free vulnerability in the HTMLFormElement::prepareForSubmission function in core/html/HTMLFormElement.cpp in Blink, as used in Google Chrome before 30.0.1599.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to submission for FORM elements.

CVE-2013-2928	Multiple unspecified vulnerabilities in Google Chrome before 30.0.1599.101 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2013-2931	Multiple unspecified vulnerabilities in Google Chrome before 31.0.1650.48 allow attackers to execute arbitrary code or possibly have other impact via unknown vectors.
CVE-2013-3210	Opera before 12.15 does not properly block top-level domains in Set-Cookie headers, which allows remote attackers to obtain sensitive information by leveraging control of a different web site in the same top-level domain.
CVE-2013-3211	Unspecified vulnerability in Opera before 12.15 has unknown impact and attack vectors, related to a "moderately severe issue."
CVE-2013-3324	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3325, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.
CVE-2013-3325	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2728, CVE-2013-3324, CVE-2013-3326, CVE-2013-3327, CVE-2013-3328, CVE-2013-3329, CVE-2013-3330, CVE-2013-3331, CVE-2013-3332, CVE-2013-3333, CVE-2013-3334, and CVE-2013-3335.
CVE-2013-3326	Adobe Flash Player before 10.3.183.86 and 11.x before 11.7.700.202 on Windows and Mac OS X, before 10.3.183.86 and 11.x before 11.2.202.285 on Linux, before 11.1.111.54 on Android 2.x and 3.x, and before 11.1.115.58 on Android 4.x; Adobe AIR before 3.7.0.1860; and Adobe AIR SDK & Compiler before 3.7.0.1860 allow attackers to execute

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

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

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

	to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, and CVE-2013-3341.
CVE-2013-3341	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-2718, CVE-2013-2719, CVE-2013-2720, CVE-2013-2721, CVE-2013-2722, CVE-2013-2723, CVE-2013-2725, CVE-2013-2726, CVE-2013-2731, CVE-2013-2732, CVE-2013-2734, CVE-2013-2735, CVE-2013-2736, CVE-2013-3337, CVE-2013-3338, CVE-2013-3339, and CVE-2013-3340.
CVE-2013-3342	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 do not properly handle operating-system domain blacklists, which has unspecified impact and attack vectors.
CVE-2013-3343	Adobe Flash Player before 10.3.183.90 and 11.x before 11.7.700.224 on Windows, before 10.3.183.90 and 11.x before 11.7.700.225 on Mac OS X, before 10.3.183.90 and 11.x before 11.2.202.291 on Linux, before 11.1.111.59 on Android 2.x and 3.x, and before 11.1.115.63 on Android 4.x; Adobe AIR before 3.7.0.2090 on Windows and Android and before 3.7.0.2100 on Mac OS X; and Adobe AIR SDK & Compiler before 3.7.0.2090 on Windows and before 3.7.0.2100 on Mac OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-3344	Heap-based buffer overflow in Adobe Flash Player before 11.7.700.232 and 11.8.x before 11.8.800.94 on Windows and Mac OS X, before 11.2.202.297 on Linux, before 11.1.111.64 on Android 2.x and 3.x, and before 11.1.115.69 on Android 4.x allows attackers to execute arbitrary code via unspecified vectors.
CVE-2013-3345	Adobe Flash Player before 11.7.700.232 and 11.8.x before 11.8.800.94 on Windows and Mac OS X, before 11.2.202.297 on Linux, before 11.1.111.64 on Android 2.x and 3.x, and before 11.1.115.69 on Android 4.x allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-3346	Adobe Reader and Acrobat 9.x before 9.5.5, 10.x before 10.1.7, and 11.x before 11.0.03 allow attackers

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

	SDK & Compiler before 3.8.0.1430 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-3361, CVE-2013-3362, and CVE-2013-3363.
CVE-2013-5329	Adobe Flash Player before 11.7.700.252 and 11.8.x and 11.9.x before 11.9.900.152 on Windows and Mac OS X and before 11.2.202.327 on Linux, Adobe AIR before 3.9.0.1210, Adobe AIR SDK before 3.9.0.1210, and Adobe AIR SDK & Compiler before 3.9.0.1210 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-5330.
CVE-2013-5330	Adobe Flash Player before 11.7.700.252 and 11.8.x and 11.9.x before 11.9.900.152 on Windows and Mac OS X and before 11.2.202.327 on Linux, Adobe AIR before 3.9.0.1210, Adobe AIR SDK before 3.9.0.1210, and Adobe AIR SDK & Compiler before 3.9.0.1210 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2013-5329.
CVE-2013-5331	Adobe Flash Player before 11.7.700.257 and 11.8.x and 11.9.x before 11.9.900.170 on Windows and Mac OS X and before 11.2.202.332 on Linux, Adobe AIR before 3.9.0.1380, Adobe AIR SDK before 3.9.0.1380, and Adobe AIR SDK & Compiler before 3.9.0.1380 allow remote attackers to execute arbitrary code via crafted .swf content that leverages an unspecified "type confusion," as exploited in the wild in December 2013.
CVE-2013-5332	Adobe Flash Player before 11.7.700.257 and 11.8.x and 11.9.x before 11.9.900.170 on Windows and Mac OS X and before 11.2.202.332 on Linux, Adobe AIR before 3.9.0.1380, Adobe AIR SDK before 3.9.0.1380, and Adobe AIR SDK & Compiler before 3.9.0.1380 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.
CVE-2013-5653	The getenv and filenameforall functions in Ghostscript 9.10 ignore the "-dSAFER" argument, which allows remote attackers to read data via a crafted postscript file.
CVE-2013-6166	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-2013-7108	Multiple off-by-one errors in Nagios Core 3.5.1, 4.0.2, and earlier, and Icinga before 1.8.5, 1.9 before 1.9.4, and 1.10 before 1.10.2 allow remote authenticated users to obtain sensitive information from process memory or cause a denial of service (crash) via a long string in the last key value in the variable list to the process_cgivars function in (1) avail.c, (2) cmd.c, (3) config.c, (4) extinfo.c, (5) histogram.c, (6) notifications.c, (7) outages.c, (8) status.c, (9) statusmap.c, (10) summary.c, and (11) trends.c in cgi/, which triggers a heap-based buffer over-read.
CVE-2013-7205	Off-by-one error in the process_cgivars function in contrib/daemonchk.c in Nagios Core 3.5.1, 4.0.2, and earlier allows remote authenticated users to obtain sensitive information from process memory or cause a denial of service (crash) via a long string in the last key value in the variable list, which triggers a heap-based buffer over-read.
CVE-2013-7447	Integer overflow in the gdk_cairo_set_source_pixbuf function in gdk/gdkcairo.c in GTK+ before 3.9.8, as

	used in eom, gnome-photos, eog, gambas3, thunar, pinpoint, and possibly other applications, allows remote attackers to cause a denial of service (crash) via a large image file, which triggers a large memory allocation.
CVE-2013-7456	gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.1.1, as used in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7, allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted image that is mishandled by the imagescale function.
CVE-2013-7459	Heap-based buffer overflow in the ALGnew function in block_templace.c in Python Cryptography Toolkit (aka pycrypto) allows remote attackers to execute arbitrary code as demonstrated by a crafted iv parameter to cryptmsg.py.
CVE-2014-0047	Docker before 1.5 allows local users to have unspecified impact via vectors involving unsafe /tmp usage.
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-2014-0791	Integer overflow in the license_read_scope_list function in libfreerdp/core/license.c in FreeRDP through 1.0.2 allows remote RDP servers to cause a denial of service (application crash) or possibly have unspecified other impact via a large ScopeCount value in a Scope List in a Server License Request packet.
CVE-2014-10070	zsh before 5.0.7 allows evaluation of the initial values of integer variables imported from the environment (instead of treating them as literal numbers). That could allow local privilege escalation, under some specific and atypical conditions where zsh is being invoked

	in privilege-elevation contexts when the environment has not been properly sanitized, such as when zsh is invoked by sudo on systems where "env_reset" has been disabled.
CVE-2014-10071	In exec.c in zsh before 5.0.7, there is a buffer overflow for very long fds in the ">& fd" syntax.
CVE-2014-10072	In utils.c in zsh before 5.0.6, there is a buffer overflow when scanning very long directory paths for symbolic links.
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-2014-1878	Stack-based buffer overflow in the cmd_submitf function in cgi/cmd.c in Nagios Core, possibly 4.0.3rc1 and earlier, and Icinga before 1.8.6, 1.9 before 1.9.5, and 1.10 before 1.10.3 allows remote attackers to cause a denial of service (segmentation fault) via a long message to cmd.cgi.
CVE-2014-2497	The gdImageCreateFromXpm function in gdxpm.c in libgd, as used in PHP 5.4.26 and earlier, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted color table in an XPM file.
CVE-2014-3120	The default configuration in Elasticsearch before 1.2 enables dynamic scripting, which allows remote attackers to execute arbitrary MVEL expressions and Java code via the source parameter to _search. NOTE: this only violates the vendor's intended security policy if the user does not run Elasticsearch in its own independent virtual machine.
CVE-2014-3152	Integer underflow in the LCodeGen::PrepareKeyedOperand function in arm/lithium-codegen-arm.cc in Google V8 before 3.25.28.16, as used in Google Chrome before 35.0.1916.114, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a negative key value.
CVE-2014-3154	Use-after-free vulnerability in the ChildThread::Shutdown function in content/child/

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

CVE-2014-3167	Multiple unspecified vulnerabilities in Google Chrome before 36.0.1985.143 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3168	Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before 37.0.2062.94, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper caching associated with animation.
CVE-2014-3169	Use-after-free vulnerability in core/dom/ ContainerNode.cpp in the DOM implementation in Blink, as used in Google Chrome before 37.0.2062.94, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging script execution that occurs before notification of node removal.
CVE-2014-3170	extensions/common/url_pattern.cc in Google Chrome before 37.0.2062.94 does not prevent use of a '\0' character in a host name, which allows remote attackers to spoof the extension permission dialog by relying on truncation after this character.
CVE-2014-3171	Use-after-free vulnerability in the V8 bindings in Blink, as used in Google Chrome before 37.0.2062.94, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper use of HashMap add operations instead of HashMap set operations, related to bindings/ core/v8/DOMWrapperMap.h and bindings/core/v8/ SerializedScriptValue.cpp.
CVE-2014-3172	The Debugger extension API in browser/extensions/api/ debugger/debugger_api.cc in Google Chrome before 37.0.2062.94 does not validate a tab's URL before an attach operation, which allows remote attackers to bypass intended access limitations via an extension that uses a restricted URL, as demonstrated by a chrome:// URL.
CVE-2014-3173	The WebGL implementation in Google Chrome before 37.0.2062.94 does not ensure that clear calls interact properly with the state of a draw buffer, which allows remote attackers to cause a denial of service (read of uninitialized memory) via a crafted CANVAS element, related to gpu/command_buffer/service/ framebuffer_manager.cc and gpu/command_buffer/ service/gles2_cmd_decoder.cc.
CVE-2014-3174	modules/webaudio/BiquadDSPKernel.cpp in the Web Audio API implementation in Blink, as used in Google Chrome before 37.0.2062.94, does not properly consider concurrent threads during attempts to update biquad filter coefficients, which allows remote attackers

	to cause a denial of service (read of uninitialized memory) via crafted API calls.
CVE-2014-3175	Multiple unspecified vulnerabilities in Google Chrome before 37.0.2062.94 allow attackers to cause a denial of service or possibly have other impact via unknown vectors, related to the load_truetype_glyph function in truetype/ttgload.c in FreeType and other functions in other components.
CVE-2014-3176	Google Chrome before 37.0.2062.94 does not properly handle the interaction of extensions, IPC, the sync API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-3177.
CVE-2014-3177	Google Chrome before 37.0.2062.94 does not properly handle the interaction of extensions, IPC, the sync API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2014-3176.
CVE-2014-3178	Use-after-free vulnerability in core/dom/Node.cpp in Blink, as used in Google Chrome before 37.0.2062.120, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging improper handling of render-tree inconsistencies.
CVE-2014-3179	Multiple unspecified vulnerabilities in Google Chrome before 37.0.2062.120 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3188	Google Chrome before 38.0.2125.101 and Chrome OS before 38.0.2125.101 do not properly handle the interaction of IPC and Google V8, which allows remote attackers to execute arbitrary code via vectors involving JSON data, related to improper parsing of an escaped index by ParseJsonObject in json-parser.h.
CVE-2014-3189	The chrome_pdf::CopyImage function in pdf/draw_utils.cc in the PDFium component in Google Chrome before 38.0.2125.101 does not properly validate image-data dimensions, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via unknown vectors.
CVE-2014-3190	Use-after-free vulnerability in the Event::currentTarget function in core/events/Event.cpp in Blink, as used in Google Chrome before 38.0.2125.101, allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via crafted JavaScript code that accesses the path property of an Event object.
CVE-2014-3191	Use-after-free vulnerability in Blink, as used in Google Chrome before 38.0.2125.101, allows remote attackers to cause a denial of service or possibly

	have unspecified other impact via crafted JavaScript code that triggers a widget-position update that improperly interacts with the render tree, related to the FrameView::updateLayoutAndStyleForPainting function in core/frame/FrameView.cpp and the RenderLayerScrollableArea::setScrollOffset function in core/rendering/RenderLayerScrollableArea.cpp.
CVE-2014-3192	Use-after-free vulnerability in the ProcessingInstruction::setXSLStyleSheet function in core/dom/ProcessingInstruction.cpp in the DOM implementation in Blink, as used in Google Chrome before 38.0.2125.101, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-3193	The SessionService::GetLastSession function in browser/sessions/session_service.cc in Google Chrome before 38.0.2125.101 allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors that leverage "type confusion" for callback processing.
CVE-2014-3194	Use-after-free vulnerability in the Web Workers implementation in Google Chrome before 38.0.2125.101 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-3195	Google V8, as used in Google Chrome before 38.0.2125.101, does not properly track JavaScript heap-memory allocations as allocations of uninitialized memory and does not properly concatenate arrays of double-precision floating-point numbers, which allows remote attackers to obtain sensitive information via crafted JavaScript code, related to the PagedSpace::AllocateRaw and NewSpace::AllocateRaw functions in heap/spaces-inl.h, the LargeObjectSpace::AllocateRaw function in heap/spaces.cc, and the Runtime_ArrayConcat function in runtime.cc.
CVE-2014-3196	base/memory/shared_memory_win.cc in Google Chrome before 38.0.2125.101 on Windows does not properly implement read-only restrictions on shared memory, which allows attackers to bypass a sandbox protection mechanism via unspecified vectors.
CVE-2014-3197	The NavigationScheduler::schedulePageBlock function in core/loader/NavigationScheduler.cpp in Blink, as used in Google Chrome before 38.0.2125.101, does not properly provide substitute data for pages blocked by the XSS auditor, which allows remote attackers to obtain sensitive information via a crafted web site.
CVE-2014-3198	The Instance::HandleInputEvent function in pdf/instance.cc in the PDFium component in Google Chrome before 38.0.2125.101 interprets a certain -1

	value as an index instead of a no-visible-page error code, which allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2014-3199	The wrap function in bindings/core/v8/custom/V8EventCustom.cpp in the V8 bindings in Blink, as used in Google Chrome before 38.0.2125.101, has an erroneous fallback outcome for wrapper-selection failures, which allows remote attackers to cause a denial of service via vectors that trigger stopping a worker process that had been handling an Event object.
CVE-2014-3200	Multiple unspecified vulnerabilities in Google Chrome before 38.0.2125.101 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-3803	The SpeechInput feature in Blink, as used in Google Chrome before 35.0.1916.114, allows remote attackers to enable microphone access and obtain speech-recognition text without indication via an INPUT element with a -x-webkit-speech attribute.
CVE-2014-4671	Adobe Flash Player before 13.0.0.231 and 14.x before 14.0.0.145 on Windows and OS X and before 11.2.202.394 on Linux, Adobe AIR before 14.0.0.137 on Android, Adobe AIR SDK before 14.0.0.137, and Adobe AIR SDK & Compiler before 14.0.0.137 do not properly restrict the SWF file format, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks against JSONP endpoints, and obtain sensitive information, via a crafted OBJECT element with SWF content satisfying the character-set requirements of a callback API.
CVE-2014-5333	Adobe Flash Player before 13.0.0.241 and 14.x before 14.0.0.176 on Windows and OS X and before 11.2.202.400 on Linux, Adobe AIR before 14.0.0.178 on Windows and OS X and before 14.0.0.179 on Android, Adobe AIR SDK before 14.0.0.178, and Adobe AIR SDK & Compiler before 14.0.0.178 do not properly restrict the SWF file format, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks against JSONP endpoints, and obtain sensitive information, via a crafted OBJECT element with SWF content satisfying the character-set requirements of a callback API, in conjunction with a manipulation involving a '$' (dollar sign) or '(' (open parenthesis) character. NOTE: this issue exists because of an incomplete fix for CVE-2014-4671.
CVE-2014-7899	Google Chrome before 38.0.2125.101 allows remote attackers to spoof the address bar by placing a blob: substring at the beginning of the URL, followed by the original URI scheme and a long username string.
CVE-2014-7900	Use-after-free vulnerability in the CPDF_Parser::IsLinearizedFile function in fpdfapi/

	fpdf_parser/fpdf_parser_parser.cpp in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.
CVE-2014-7901	Integer overflow in the opj_t2_read_packet_data function in fxcodec/fx_libopenjpeg/libopenjpeg20/t2.c in OpenJPEG in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a long segment in a JPEG image.
CVE-2014-7902	Use-after-free vulnerability in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.
CVE-2014-7903	Buffer overflow in OpenJPEG before r2911 in PDFium, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted JPEG image.
CVE-2014-7904	Buffer overflow in Skia, as used in Google Chrome before 39.0.2171.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-7906	Use-after-free vulnerability in the Pepper plugins in Google Chrome before 39.0.2171.65 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted Flash content that triggers an attempted PepperMediaDeviceManager access outside of the object's lifetime.
CVE-2014-7907	Multiple use-after-free vulnerabilities in modules/screen_orientation/ScreenOrientationController.cpp in Blink, as used in Google Chrome before 39.0.2171.65, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger improper handling of a detached frame, related to the (1) lock and (2) unlock methods.
CVE-2014-7908	Multiple integer overflows in the CheckMov function in media/base/container_names.cc in Google Chrome before 39.0.2171.65 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a large atom in (1) MPEG-4 or (2) QuickTime .mov data.
CVE-2014-7909	effects/SkDashPathEffect.cpp in Skia, as used in Google Chrome before 39.0.2171.65, computes a hash key using uninitialized integer values, which might allow remote attackers to cause a denial of service by rendering crafted data.
CVE-2014-7910	Multiple unspecified vulnerabilities in Google Chrome before 39.0.2171.65 allow attackers to cause a denial

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

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

CVE-2014-7937	Multiple off-by-one errors in libavcodec/vorbisdec.c in FFmpeg before 2.4.2, as used in Google Chrome before 40.0.2214.91, allow remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted Vorbis I data.
CVE-2014-7938	The Fonts implementation in Google Chrome before 40.0.2214.91 allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2014-7939	Google Chrome before 40.0.2214.91, when the Harmony proxy in Google V8 is enabled, allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code with Proxy.create and console.log calls, related to HTTP responses that lack an "X-Content-Type-Options: nosniff" header.
CVE-2014-7940	The collator implementation in i18n/ucol.cpp in International Components for Unicode (ICU) 52 through SVN revision 293126, as used in Google Chrome before 40.0.2214.91, does not initialize memory for a data structure, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted character sequence.
CVE-2014-7941	The SelectionOwner::ProcessTarget function in ui/base/x/selection_owner.cc in the UI implementation in Google Chrome before 40.0.2214.91 uses an incorrect data type for a certain length value, which allows remote attackers to cause a denial of service (out-of-bounds read) via crafted X11 data.
CVE-2014-7942	The Fonts implementation in Google Chrome before 40.0.2214.91 does not initialize memory for a data structure, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2014-7943	Skia, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2014-7944	The sycc422_to_rgb function in fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 40.0.2214.91, does not properly handle odd values of image width, which allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document.
CVE-2014-7945	OpenJPEG before r2908, as used in PDFium in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document, related to j2k.c, jp2.c, and t2.c.
CVE-2014-7946	The RenderTable::simplifiedNormalFlowLayout function in core/rendering/RenderTable.cpp in Blink, as used in Google Chrome before 40.0.2214.91, skips captions during table layout in certain situations, which allows

	remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors related to the Fonts implementation.
CVE-2014-7947	OpenJPEG before r2944, as used in PDFium in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted PDF document, related to j2k.c, jp2.c, pi.c, t1.c, t2.c, and tcd.c.
CVE-2014-7948	The AppCacheUpdateJob::URLFetcher::OnResponseStarted function in content/browser/appcache/appcache_update_job.cc in Google Chrome before 40.0.2214.91 proceeds with AppCache caching for SSL sessions even if there is an X.509 certificate error, which allows man-in-the-middle attackers to spoof HTML5 application content via a crafted certificate.
CVE-2014-7967	Multiple unspecified vulnerabilities in Google V8 before 3.28.71.15, as used in Google Chrome before 38.0.2125.101, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2014-8354	The HorizontalFilter function in resize.c in ImageMagick before 6.8.9-9 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted image file.
CVE-2014-8355	PCX parser code in ImageMagick before 6.8.9-9 allows remote attackers to cause a denial of service (out-of-bounds read).
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-2014-8562	DCM decode in ImageMagick before 6.8.9-9 allows remote attackers to cause a denial of service (out-of-bounds read).
CVE-2014-8716	The JPEG decoder in ImageMagick before 6.8.9-9 allows local users to cause a denial of service (out-of-bounds memory access and crash).
CVE-2014-9092	libjpeg-turbo before 1.3.1 allows remote attackers to cause a denial of service (crash) via a crafted JPEG file, related to the Exif marker.
CVE-2014-9162	Adobe Flash Player before 13.0.0.259 and 14.x through 16.x before 16.0.0.235 on Windows and OS X and before 11.2.202.425 on Linux allows attackers to obtain sensitive information via unspecified vectors.
CVE-2014-9163	Stack-based buffer overflow in Adobe Flash Player before 13.0.0.259 and 14.x and 15.x before 15.0.0.246 on Windows and OS X and before 11.2.202.425 on Linux allows attackers to execute arbitrary code

	via unspecified vectors, as exploited in the wild in December 2014.
CVE-2014-9164	Adobe Flash Player before 13.0.0.259 and 14.x through 16.x before 16.0.0.235 on Windows and OS X and before 11.2.202.425 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2014-0587.
CVE-2014-9620	The ELF parser in file 5.08 through 5.21 allows remote attackers to cause a denial of service via a large number of notes.
CVE-2014-9621	The ELF parser in file 5.16 through 5.21 allows remote attackers to cause a denial of service via a long string.
CVE-2014-9646	Unquoted Windows search path vulnerability in the GoogleChromeDistribution::DoPostUninstallOperations function in installer/util/google_chrome_distribution.cc in the uninstall-survey feature in Google Chrome before 40.0.2214.91 allows local users to gain privileges via a Trojan horse program in the %SYSTEMDRIVE% directory, as demonstrated by program.exe, a different vulnerability than CVE-2015-1205.
CVE-2014-9647	Use-after-free vulnerability in PDFium, as used in Google Chrome before 40.0.2214.91, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document, related to fpdfsdk/src/fpdfview.cpp and fpdfsdk/src/fsdk_mgr.cpp, a different vulnerability than CVE-2015-1205.
CVE-2014-9653	readelf.c in file before 5.22, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not consider that pread calls sometimes read only a subset of the available data, which allows remote attackers to cause a denial of service (uninitialized memory access) or possibly have unspecified other impact via a crafted ELF file.
CVE-2014-9654	The Regular Expressions package in International Components for Unicode (ICU) for C/C++ before 2014-12-03, as used in Google Chrome before 40.0.2214.91, calculates certain values without ensuring that they can be represented in a 24-bit field, which allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a crafted string, a related issue to CVE-2014-7923.
CVE-2014-9689	content/renderer/device_sensors/device_orientation_event_pump.cc in Google Chrome before 41.0.2272.76 does not properly restrict access to high-rate gyroscope data, which makes it easier for remote attackers to obtain speech signals from a device's physical environment via a crafted web site

	that listens for ondeviceorientation events, a different vulnerability than CVE-2015-1231.
CVE-2014-9709	The GetCode_ function in gd_gif_in.c in GD 2.1.1 and earlier, as used in PHP before 5.5.21 and 5.6.x before 5.6.5, allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted GIF image that is improperly handled by the gdImageCreateFromGif function.
CVE-2014-9771	Integer overflow in imlib2 before 1.4.7 allows remote attackers to cause a denial of service (memory consumption or application crash) via a crafted image, which triggers an invalid read operation.
CVE-2014-9805	ImageMagick allows remote attackers to cause a denial of service (segmentation fault and application crash) via a crafted pnm file.
CVE-2014-9806	ImageMagick allows remote attackers to cause a denial of service (file descriptor consumption) via a crafted file.
CVE-2014-9807	The pdb coder in ImageMagick allows remote attackers to cause a denial of service (double free) via unspecified vectors.
CVE-2014-9808	ImageMagick allows remote attackers to cause a denial of service (segmentation fault and application crash) via a crafted dpc image.
CVE-2014-9809	ImageMagick allows remote attackers to cause a denial of service (segmentation fault and application crash) via a crafted xwd image.
CVE-2014-9810	The dpx file handler in ImageMagick allows remote attackers to cause a denial of service (segmentation fault and application crash) via a malformed dpx file.
CVE-2014-9811	The xwd file handler in ImageMagick allows remote attackers to cause a denial of service (segmentation fault and application crash) via a malformed xwd file.
CVE-2014-9812	ImageMagick allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted ps file.
CVE-2014-9813	ImageMagick allows remote attackers to cause a denial of service (application crash) via a crafted viff file.
CVE-2014-9814	ImageMagick allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted wpg file.
CVE-2014-9815	ImageMagick allows remote attackers to cause a denial of service (application crash) via a crafted wpg file.
CVE-2014-9816	ImageMagick allows remote attackers to cause a denial of service (out-of-bounds access) via a crafted viff file.
CVE-2014-9817	Heap-based buffer overflow in ImageMagick allows remote attackers to have unspecified impact via a crafted pdb file.

CVE-2014-9818	ImageMagick allows remote attackers to cause a denial of service (out-of-bounds access) via a malformed sun file.
CVE-2014-9819	Heap-based buffer overflow in ImageMagick allows remote attackers to have unspecified impact via a crafted palm file, a different vulnerability than CVE-2014-9823.
CVE-2014-9820	Heap-based buffer overflow in ImageMagick allows remote attackers to have unspecified impact via a crafted pnm file.
CVE-2014-9821	Heap-based buffer overflow in ImageMagick allows remote attackers to have unspecified impact via a crafted xpm file.
CVE-2014-9822	Heap-based buffer overflow in ImageMagick allows remote attackers to have unspecified impact via a crafted quantum file.
CVE-2014-9823	Heap-based buffer overflow in ImageMagick allows remote attackers to have unspecified impact via a crafted palm file, a different vulnerability than CVE-2014-9819.
CVE-2014-9826	ImageMagick allows remote attackers to have unspecified impact via vectors related to error handling in sun files.
CVE-2014-9828	coders/psd.c in ImageMagick allows remote attackers to have unspecified impact via a crafted psd file.
CVE-2014-9829	coders/sun.c in ImageMagick allows remote attackers to cause a denial of service (out-of-bounds access) via a crafted sun file.
CVE-2014-9830	coders/sun.c in ImageMagick allows remote attackers to have unspecified impact via a corrupted sun file.
CVE-2014-9831	coders/wpg.c in ImageMagick allows remote attackers to have unspecified impact via a corrupted wpg file.
CVE-2014-9833	Heap overflow in ImageMagick 6.8.9-9 via a crafted psd file.
CVE-2014-9834	Heap overflow in ImageMagick 6.8.9-9 via a crafted pict file.
CVE-2014-9835	Heap overflow in ImageMagick 6.8.9-9 via a crafted wpf file.
CVE-2014-9836	ImageMagick 6.8.9-9 allows remote attackers to cause a denial of service via a crafted xpm file.
CVE-2014-9837	coders/pnm.c in ImageMagick 6.9.0-1 Beta and earlier allows remote attackers to cause a denial of service (crash) via a crafted png file.
CVE-2014-9838	magick/cache.c in ImageMagick 6.8.9-9 allows remote attackers to cause a denial of service (crash).

CVE-2014-9839	magick/colormap-private.h in ImageMagick 6.8.9-9 allows remote attackers to cause a denial of service (out-of-bounds access).
CVE-2014-9840	ImageMagick 6.8.9-9 allows remote attackers to cause a denial of service (out-of-bounds access) via a crafted palm file.
CVE-2014-9841	The ReadPSDLayers function in coders/psd.c in ImageMagick 6.8.9.9 allows remote attackers to have unspecified impact via unknown vectors, related to "throwing of exceptions."
CVE-2014-9843	The DecodePSDPixels function in coders/psd.c in ImageMagick 6.8.9.9 allows remote attackers to have unspecified impact via unknown vectors.
CVE-2014-9844	The ReadRLEImage function in coders/rle.c in ImageMagick 6.8.9.9 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted image file.
CVE-2014-9845	The ReadDIBImage function in coders/dib.c in ImageMagick allows remote attackers to cause a denial of service (crash) via a corrupted dib file.
CVE-2014-9900	The ethtool_get_wol function in net/core/ethtool.c in the Linux kernel through 4.7, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not initialize a certain data structure, which allows local users to obtain sensitive information via a crafted application, aka Android internal bug 28803952 and Qualcomm internal bug CR570754.
CVE-2014-9911	Stack-based buffer overflow in the ures_getByKeyWithFallback function in common/uresbund.cpp in International Components for Unicode (ICU) before 54.1 for C/C++ allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted uloc_getDisplayName call.
CVE-2015-0245	D-Bus 1.4.x through 1.6.x before 1.6.30, 1.8.x before 1.8.16, and 1.9.x before 1.9.10 does not validate the source of ActivationFailure signals, which allows local users to cause a denial of service (activation failure error returned) by leveraging a race condition involving sending an ActivationFailure signal before systemd responds.
CVE-2015-0301	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 do not properly validate files, which has unspecified impact and attack vectors.

CVE-2015-0302	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allow attackers to obtain sensitive keystroke information via unspecified vectors.
CVE-2015-0303	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0306.
CVE-2015-0304	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0309.
CVE-2015-0305	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion."
CVE-2015-0306	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0303.
CVE-2015-0307	Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before

	16.0.0.272 allow remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2015-0308	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-0309	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.260 and 14.x through 16.x before 16.0.0.257 on Windows and OS X and before 11.2.202.429 on Linux, Adobe AIR before 16.0.0.245 on Windows and OS X and before 16.0.0.272 on Android, Adobe AIR SDK before 16.0.0.272, and Adobe AIR SDK & Compiler before 16.0.0.272 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0304.
CVE-2015-0310	Adobe Flash Player before 13.0.0.262 and 14.x through 16.x before 16.0.0.287 on Windows and OS X and before 11.2.202.438 on Linux does not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism on Windows, and have an unspecified impact on other platforms, via unknown vectors, as exploited in the wild in January 2015.
CVE-2015-0311	Unspecified vulnerability in Adobe Flash Player through 13.0.0.262 and 14.x, 15.x, and 16.x through 16.0.0.287 on Windows and OS X and through 11.2.202.438 on Linux allows remote attackers to execute arbitrary code via unknown vectors, as exploited in the wild in January 2015.
CVE-2015-0312	Double free vulnerability in Adobe Flash Player before 13.0.0.264 and 14.x through 16.x before 16.0.0.296 on Windows and OS X and before 11.2.202.440 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-0313	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows remote attackers to execute arbitrary code via unspecified vectors, as exploited in the wild in February 2015, a different vulnerability than CVE-2015-0315, CVE-2015-0320, and CVE-2015-0322.
CVE-2015-0314	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code or cause a denial

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

	vectors, a different vulnerability than CVE-2015-0314, CVE-2015-0316, CVE-2015-0318, CVE-2015-0329, and CVE-2015-0330.
CVE-2015-0322	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0313, CVE-2015-0315, and CVE-2015-0320.
CVE-2015-0323	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0327.
CVE-2015-0324	Buffer overflow in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-0325	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2015-0326 and CVE-2015-0328.
CVE-2015-0326	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2015-0325 and CVE-2015-0328.
CVE-2015-0327	Heap-based buffer overflow in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0323.
CVE-2015-0328	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to cause a denial of service (NULL pointer dereference) or possibly have unspecified other impact via unknown vectors, a different vulnerability than CVE-2015-0325 and CVE-2015-0326.
CVE-2015-0329	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and

	OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0314, CVE-2015-0316, CVE-2015-0318, CVE-2015-0321, and CVE-2015-0330.
CVE-2015-0330	Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0314, CVE-2015-0316, CVE-2015-0318, CVE-2015-0321, and CVE-2015-0329.
CVE-2015-0331	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.269 and 14.x through 16.x before 16.0.0.305 on Windows and OS X and before 11.2.202.442 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0313, CVE-2015-0315, CVE-2015-0320, and CVE-2015-0322.
CVE-2015-0332	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0333, CVE-2015-0335, and CVE-2015-0339.
CVE-2015-0333	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0332, CVE-2015-0335, and CVE-2015-0339.
CVE-2015-0334	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-0336.
CVE-2015-0335	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0332, CVE-2015-0333, and CVE-2015-0339.
CVE-2015-0336	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows

	attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-0334.
CVE-2015-0337	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2015-0338	Integer overflow in Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-0339	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0332, CVE-2015-0333, and CVE-2015-0335.
CVE-2015-0340	Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows remote attackers to bypass intended file-upload restrictions via unspecified vectors.
CVE-2015-0341	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0342.
CVE-2015-0342	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.277 and 14.x through 17.x before 17.0.0.134 on Windows and OS X and before 11.2.202.451 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0341.
CVE-2015-0346	Double free vulnerability in Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0359.
CVE-2015-0347	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0350, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355,

	CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, CVE-2015-3042, and CVE-2015-3043.
CVE-2015-0348	Buffer overflow in Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-0349	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0351, CVE-2015-0358, and CVE-2015-3039.
CVE-2015-0350	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0347, CVE-2015-0352, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, CVE-2015-3042, and CVE-2015-3043.
CVE-2015-0351	Use-after-free vulnerability in Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-0349, CVE-2015-0358, and CVE-2015-3039.
CVE-2015-0352	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0347, CVE-2015-0350, CVE-2015-0353, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, CVE-2015-3042, and CVE-2015-3043.
CVE-2015-0353	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-0347, CVE-2015-0350, CVE-2015-0352, CVE-2015-0354, CVE-2015-0355, CVE-2015-0360, CVE-2015-3038, CVE-2015-3041, CVE-2015-3042, and CVE-2015-3043.
CVE-2015-0354	Adobe Flash Player before 13.0.0.281 and 14.x through 17.x before 17.0.0.169 on Windows and OS X and before 11.2.202.457 on Linux allows attackers to

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

	of service or possibly have other impact via unknown vectors.
CVE-2015-1209	Use-after-free vulnerability in the VisibleSelection::nonBoundaryShadowTreeRootNode function in core/editing/VisibleSelection.cpp in the DOM implementation in Blink, as used in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers improper handling of a shadow-root anchor.
CVE-2015-1210	The V8ThrowException::createDOMException function in bindings/core/v8/V8ThrowException.cpp in the V8 bindings in Blink, as used in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android, does not properly consider frame access restrictions during the throwing of an exception, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2015-1211	The OriginCanAccessServiceWorkers function in content/browser/service_worker/service_worker_dispatcher_host.cc in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android does not properly restrict the URI scheme during a ServiceWorker registration, which allows remote attackers to gain privileges via a filesystem: URI.
CVE-2015-1212	Multiple unspecified vulnerabilities in Google Chrome before 40.0.2214.111 on Windows, OS X, and Linux and before 40.0.2214.109 on Android allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1213	The SkBitmap::ReadRawPixels function in core/SkBitmap.cpp in the filters implementation in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an out-of-bounds write operation.
CVE-2015-1214	Integer overflow in the SkAutoSTArray implementation in include/core/SkTemplates.h in the filters implementation in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a reset action with a large count value, leading to an out-of-bounds write operation.
CVE-2015-1215	The filters implementation in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have

	unspecified other impact via vectors that trigger an out-of-bounds write operation.
CVE-2015-1216	Use-after-free vulnerability in the V8Window::namedPropertyGetterCustom function in bindings/core/v8/custom/V8WindowCustom.cpp in the V8 bindings in Blink, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger a frame detachment.
CVE-2015-1217	The V8LazyEventListener::prepareListenerObject function in bindings/core/v8/V8LazyEventListener.cpp in the V8 bindings in Blink, as used in Google Chrome before 41.0.2272.76, does not properly compile listeners, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2015-1218	Multiple use-after-free vulnerabilities in the DOM implementation in Blink, as used in Google Chrome before 41.0.2272.76, allow remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger movement of a SCRIPT element to different documents, related to (1) the HTMLScriptElement::didMoveToNewDocument function in core/html/HTMLScriptElement.cpp and (2) the SVGScriptElement::didMoveToNewDocument function in core/svg/SVGScriptElement.cpp.
CVE-2015-1219	Integer overflow in the SkMallocPixelRef::NewAllocate function in core/SkMallocPixelRef.cpp in Skia, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that trigger an attempted allocation of a large amount of memory during WebGL rendering.
CVE-2015-1220	Use-after-free vulnerability in the GIFImageReader::parseData function in platform/image-decoders/gif/GIFImageReader.cpp in Blink, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted frame size in a GIF image.
CVE-2015-1221	Use-after-free vulnerability in Blink, as used in Google Chrome before 41.0.2272.76, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect ordering of operations in the Web SQL Database thread relative to Blink's main thread, related to the shutdown function in web/WebKit.cpp.
CVE-2015-1222	Multiple use-after-free vulnerabilities in the ServiceWorkerScriptCacheMap implementation in content/browser/service_worker/service_worker_script_cache_map.cc in Google

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

	allows remote proxy servers to conduct cookie-injection attacks via a crafted response.
CVE-2015-1230	The getHiddenProperty function in bindings/core/v8/V8EventListenerList.h in Blink, as used in Google Chrome before 41.0.2272.76, has a name conflict with the AudioContext class, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via JavaScript code that adds an AudioContext event listener and triggers "type confusion."
CVE-2015-1231	Multiple unspecified vulnerabilities in Google Chrome before 41.0.2272.76 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1232	Array index error in the MidiManagerUsb::DispatchSendMidiData function in media/midi/midi_manager_usb.cc in Google Chrome before 41.0.2272.76 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging renderer access to provide an invalid port index that triggers an out-of-bounds write operation, a different vulnerability than CVE-2015-1212.
CVE-2015-1233	Google Chrome before 41.0.2272.118 does not properly handle the interaction of IPC, the Gamepad API, and Google V8, which allows remote attackers to execute arbitrary code via unspecified vectors.
CVE-2015-1234	Race condition in gpu/command_buffer/service/gles2_cmd_decoder.cc in Google Chrome before 41.0.2272.118 allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact by manipulating OpenGL ES commands.
CVE-2015-1235	The ContainerNode::parserRemoveChild function in core/dom/ContainerNode.cpp in the HTML parser in Blink, as used in Google Chrome before 42.0.2311.90, allows remote attackers to bypass the Same Origin Policy via a crafted HTML document with an IFRAME element.
CVE-2015-1236	The MediaElementAudioSourceNode::process function in modules/webaudio/MediaElementAudioSourceNode.cpp in the Web Audio API implementation in Blink, as used in Google Chrome before 42.0.2311.90, allows remote attackers to bypass the Same Origin Policy and obtain sensitive audio sample values via a crafted web site containing a media element.
CVE-2015-1237	Use-after-free vulnerability in the RenderFrameImpl::OnMessageReceived function in content/renderer/render_frame_impl.cc in Google Chrome before 42.0.2311.90 allows remote attackers to

	cause a denial of service or possibly have unspecified other impact via vectors that trigger renderer IPC messages during a detach operation.
CVE-2015-1238	Skia, as used in Google Chrome before 42.0.2311.90, allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via unknown vectors.
CVE-2015-1240	gpu/blink/webgraphicscontext3d_impl.cc in the WebGL implementation in Google Chrome before 42.0.2311.90 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WebGL program that triggers a state inconsistency.
CVE-2015-1241	Google Chrome before 42.0.2311.90 does not properly consider the interaction of page navigation with the handling of touch events and gesture events, which allows remote attackers to trigger unintended UI actions via a crafted web site that conducts a "tapjacking" attack.
CVE-2015-1242	The ReduceTransitionElementsKind function in hydrogen-check-elimination.cc in Google V8 before 4.2.77.8, as used in Google Chrome before 42.0.2311.90, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that leverages "type confusion" in the check-elimination optimization.
CVE-2015-1243	Use-after-free vulnerability in the MutationObserver::disconnect function in core/dom/MutationObserver.cpp in the DOM implementation in Blink, as used in Google Chrome before 42.0.2311.135, allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering an attempt to unregister a MutationObserver object that is not currently registered.
CVE-2015-1244	The URLRequest::GetHSTSRedirect function in url_request/url_request.cc in Google Chrome before 42.0.2311.90 does not replace the ws scheme with the wss scheme whenever an HSTS Policy is active, which makes it easier for remote attackers to obtain sensitive information by sniffing the network for WebSocket traffic.
CVE-2015-1245	Use-after-free vulnerability in the OpenPDFInReaderView::Update function in browser/ui/views/location_bar/open_pdf_in_reader_view.cc in Google Chrome before 41.0.2272.76 might allow user-assisted remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by triggering interaction with a PDFium "Open PDF in Reader" button that has an invalid tab association.

CVE-2015-1246	Blink, as used in Google Chrome before 42.0.2311.90, allows remote attackers to cause a denial of service (out-of-bounds read) via unspecified vectors.
CVE-2015-1247	The SearchEngineTabHelper::OnPageHasOSDD function in browser/ui/search_engines/ search_engine_tab_helper.cc in Google Chrome before 42.0.2311.90 does not prevent use of a file: URL for an OpenSearch descriptor XML document, which might allow remote attackers to obtain sensitive information from local files via a crafted (1) http or (2) https web site.
CVE-2015-1248	The FileSystem API in Google Chrome before 40.0.2214.91 allows remote attackers to bypass the SafeBrowsing for Executable Files protection mechanism by creating a .exe file in a temporary filesystem and then referencing this file with a filesystem:http: URL.
CVE-2015-1249	Multiple unspecified vulnerabilities in Google Chrome before 42.0.2311.90 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1250	Multiple unspecified vulnerabilities in Google Chrome before 42.0.2311.135 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1251	Use-after-free vulnerability in the SpeechRecognitionClient implementation in the Speech subsystem in Google Chrome before 43.0.2357.65 allows remote attackers to execute arbitrary code via a crafted document.
CVE-2015-1252	common/partial_circular_buffer.cc in Google Chrome before 43.0.2357.65 does not properly handle wraps, which allows remote attackers to bypass a sandbox protection mechanism or cause a denial of service (out-of-bounds write) via vectors that trigger a write operation with a large amount of data, related to the PartialCircularBuffer::Write and PartialCircularBuffer::DoWrite functions.
CVE-2015-1253	core/html/parser/HTMLConstructionSite.cpp in the DOM implementation in Blink, as used in Google Chrome before 43.0.2357.65, allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code that appends a child to a SCRIPT element, related to the insert and executeReparentTask functions.
CVE-2015-1254	core/dom/Document.cpp in Blink, as used in Google Chrome before 43.0.2357.65, enables the inheritance of the designMode attribute, which allows remote attackers to bypass the Same Origin Policy by leveraging the availability of editing.

CVE-2015-1255	Use-after-free vulnerability in content/renderer/media/webaudio_capturer_source.cc in the WebAudio implementation in Google Chrome before 43.0.2357.65 allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by leveraging improper handling of a stop action for an audio track.
CVE-2015-1256	Use-after-free vulnerability in the SVG implementation in Blink, as used in Google Chrome before 43.0.2357.65, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted document that leverages improper handling of a shadow tree for a use element.
CVE-2015-1257	platform/graphics/filters/FEColorMatrix.cpp in the SVG implementation in Blink, as used in Google Chrome before 43.0.2357.65, does not properly handle an insufficient number of values in an feColorMatrix filter, which allows remote attackers to cause a denial of service (container overflow) or possibly have unspecified other impact via a crafted document.
CVE-2015-1258	Google Chrome before 43.0.2357.65 relies on libvpx code that was not built with an appropriate --size-limit value, which allows remote attackers to trigger a negative value for a size field, and consequently cause a denial of service or possibly have unspecified other impact, via a crafted frame size in VP9 video data.
CVE-2015-1259	PDFium, as used in Google Chrome before 43.0.2357.65, does not properly initialize memory, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2015-1260	Multiple use-after-free vulnerabilities in content/renderer/media/user_media_client_impl.cc in the WebRTC implementation in Google Chrome before 43.0.2357.65 allow remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that executes upon completion of a getUserMedia request.
CVE-2015-1262	platform/fonts/shaping/HarfBuzzShaper.cpp in Blink, as used in Google Chrome before 43.0.2357.65, does not initialize a certain width field, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted Unicode text.
CVE-2015-1263	The Spellcheck API implementation in Google Chrome before 43.0.2357.65 does not use an HTTPS session for downloading a Hunspell dictionary, which allows man-in-the-middle attackers to deliver incorrect spelling suggestions or possibly have unspecified other impact via a crafted file.

CVE-2015-1264	Cross-site scripting (XSS) vulnerability in Google Chrome before 43.0.2357.65 allows user-assisted remote attackers to inject arbitrary web script or HTML via crafted data that is improperly handled by the Bookmarks feature.
CVE-2015-1265	Multiple unspecified vulnerabilities in Google Chrome before 43.0.2357.65 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1266	content/browser/webui/content_web_ui_controller_factory.cc in Google Chrome before 43.0.2357.130 does not properly consider the scheme in determining whether a URL is associated with a WebUI SiteInstance, which allows remote attackers to bypass intended access restrictions via a similar URL, as demonstrated by use of http://gpu when there is a WebUI class for handling chrome://gpu requests.
CVE-2015-1267	Blink, as used in Google Chrome before 43.0.2357.130, does not properly restrict the creation context during creation of a DOM wrapper, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code that uses a Blink public API, related to WebArrayBufferConverter.cpp, WebBlob.cpp, WebDOMError.cpp, and WebDOMFileSystem.cpp.
CVE-2015-1268	bindings/scripts/v8_types.py in Blink, as used in Google Chrome before 43.0.2357.130, does not properly select a creation context for a return value's DOM wrapper, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code, as demonstrated by use of a data: URL.
CVE-2015-1269	The DecodeHSTSPreloadRaw function in net/http/transport_security_state.cc in Google Chrome before 43.0.2357.130 does not properly canonicalize DNS hostnames before making comparisons to HSTS or HPKP preload entries, which allows remote attackers to bypass intended access restrictions via a string that (1) ends in a . (dot) character or (2) is not entirely lowercase.
CVE-2015-1270	The ucnv_io_getConverterName function in common/ucnv_io.cpp in International Components for Unicode (ICU), as used in Google Chrome before 44.0.2403.89, mishandles converter names with initial x- substrings, which allows remote attackers to cause a denial of service (read of uninitialized memory) or possibly have unspecified other impact via a crafted file.
CVE-2015-1271	PDFium, as used in Google Chrome before 44.0.2403.89, does not properly handle certain out-of-memory conditions, which allows remote attackers to cause a denial of service (heap-based buffer overflow)

	or possibly have unspecified other impact via a crafted PDF document that triggers a large memory allocation.
CVE-2015-1272	Use-after-free vulnerability in the GPU process implementation in Google Chrome before 44.0.2403.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging the continued availability of a GPUChannelHost data structure during Blink shutdown, related to content/browser/gpu/browser_gpu_channel_host_factory.cc and content/renderer/render_thread_impl.cc.
CVE-2015-1273	Heap-based buffer overflow in j2k.c in OpenJPEG before r3002, as used in PDFium in Google Chrome before 44.0.2403.89, allows remote attackers to cause a denial of service or possibly have unspecified other impact via invalid JPEG2000 data in a PDF document.
CVE-2015-1274	Google Chrome before 44.0.2403.89 does not ensure that the auto-open list omits all dangerous file types, which makes it easier for remote attackers to execute arbitrary code by providing a crafted file and leveraging a user's previous "Always open files of this type" choice, related to download_commands.cc and download_prefs.cc.
CVE-2015-1276	Use-after-free vulnerability in content/browser/indexed_db/indexed_db_backing_store.cc in the IndexedDB implementation in Google Chrome before 44.0.2403.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging an abort action before a certain write operation.
CVE-2015-1277	Use-after-free vulnerability in the accessibility implementation in Google Chrome before 44.0.2403.89 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging lack of certain validity checks for accessibility-tree data structures.
CVE-2015-1278	content/browser/web_contents/web_contents_impl.cc in Google Chrome before 44.0.2403.89 does not ensure that a PDF document's modal dialog is closed upon navigation to an interstitial page, which allows remote attackers to spoof URLs via a crafted document, as demonstrated by the alert_dialog.pdf document.
CVE-2015-1279	Integer overflow in the CJBig2_Image::expand function in fxcodec/jbig2/JBig2_Image.cpp in PDFium, as used in Google Chrome before 44.0.2403.89, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via large height and stride values.
CVE-2015-1280	SkPictureShader.cpp in Skia, as used in Google Chrome before 44.0.2403.89, allows remote attackers to cause a denial of service (memory corruption) or

	possibly have unspecified other impact by leveraging access to a renderer process and providing crafted serialized data.
CVE-2015-1281	core/loader/ImageLoader.cpp in Blink, as used in Google Chrome before 44.0.2403.89, does not properly determine the V8 context of a microtask, which allows remote attackers to bypass Content Security Policy (CSP) restrictions by providing an image from an unintended source.
CVE-2015-1282	Multiple use-after-free vulnerabilities in fpdfsdk/src/javascript/Document.cpp in PDFium, as used in Google Chrome before 44.0.2403.89, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document, related to the (1) Document::delay and (2) Document::DoFieldDelay functions.
CVE-2015-1283	Multiple integer overflows in the XML_GetBuffer function in Expat through 2.1.0, as used in Google Chrome before 44.0.2403.89 and other products, allow remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted XML data, a related issue to CVE-2015-2716.
CVE-2015-1284	The LocalFrame::isURLAllowed function in core/frame/LocalFrame.cpp in Blink, as used in Google Chrome before 44.0.2403.89, does not properly check for a page's maximum number of frames, which allows remote attackers to cause a denial of service (invalid count value and use-after-free) or possibly have unspecified other impact via crafted JavaScript code that makes many createElement calls for IFRAME elements.
CVE-2015-1285	The XSSAuditor::canonicalize function in core/html/parser/XSSAuditor.cpp in the XSS auditor in Blink, as used in Google Chrome before 44.0.2403.89, does not properly choose a truncation point, which makes it easier for remote attackers to obtain sensitive information via an unspecified linear-time attack.
CVE-2015-1286	Cross-site scripting (XSS) vulnerability in the V8ContextNativeHandler::GetModuleSystem function in extensions/renderer/v8_context_native_handler.cc in Google Chrome before 44.0.2403.89 allows remote attackers to inject arbitrary web script or HTML by leveraging the lack of a certain V8 context restriction, aka a Blink "Universal XSS (UXSS)."
CVE-2015-1287	Blink, as used in Google Chrome before 44.0.2403.89, enables a quirks-mode exception that limits the cases in which a Cascading Style Sheets (CSS) document is required to have the text/css content type, which allows remote attackers to bypass the Same Origin

	Policy via a crafted web site, related to core/fetch/CSSStyleSheetResource.cpp.
CVE-2015-1288	The Spellcheck API implementation in Google Chrome before 44.0.2403.89 does not use an HTTPS session for downloading a Hunspell dictionary, which allows man-in-the-middle attackers to deliver incorrect spelling suggestions or possibly have unspecified other impact via a crafted file, a related issue to CVE-2015-1263.
CVE-2015-1289	Multiple unspecified vulnerabilities in Google Chrome before 44.0.2403.89 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1290	The Google V8 engine, as used in Google Chrome before 44.0.2403.89 and QtWebEngineCore in Qt before 5.5.1, allows remote attackers to cause a denial of service (memory corruption) or execute arbitrary code via a crafted web site.
CVE-2015-1291	The ContainerNode::parserRemoveChild function in core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 45.0.2454.85, does not check whether a node is expected, which allows remote attackers to bypass the Same Origin Policy or cause a denial of service (DOM tree corruption) via a web site with crafted JavaScript code and IFRAME elements.
CVE-2015-1292	The NavigatorServiceWorker::serviceWorker function in modules/serviceworkers/NavigatorServiceWorker.cpp in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to bypass the Same Origin Policy by accessing a Service Worker.
CVE-2015-1293	The DOM implementation in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to bypass the Same Origin Policy via unspecified vectors.
CVE-2015-1294	Use-after-free vulnerability in the SkMatrix::invertNonIdentity function in core/SkMatrix.cpp in Skia, as used in Google Chrome before 45.0.2454.85, allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering the use of matrix elements that lead to an infinite result during an inversion calculation.
CVE-2015-1295	Multiple use-after-free vulnerabilities in the PrintWebViewHelper class in components/printing/renderer/print_web_view_helper.cc in Google Chrome before 45.0.2454.85 allow user-assisted remote attackers to cause a denial of service or possibly have unspecified other impact by triggering nested IPC messages during preparation for printing, as demonstrated by messages associated with PDF documents in conjunction with messages about printer capabilities.

CVE-2015-1296	The UnescapeURLWithAdjustmentsImpl implementation in net/base/escape.cc in Google Chrome before 45.0.2454.85 does not prevent display of Unicode LOCK characters in the omnibox, which makes it easier for remote attackers to spoof the SSL lock icon by placing one of these characters at the end of a URL, as demonstrated by the omnibox in localizations for right-to-left languages.
CVE-2015-1297	The WebRequest API implementation in extensions/browser/api/web_request/web_request_api.cc in Google Chrome before 45.0.2454.85 does not properly consider a request's source before accepting the request, which allows remote attackers to bypass intended access restrictions via a crafted (1) app or (2) extension.
CVE-2015-1298	The RuntimeEventRouter::OnExtensionUninstalled function in extensions/browser/api/runtime/runtime_api.cc in Google Chrome before 45.0.2454.85 does not ensure that the setUninstallURL preference corresponds to the URL of a web site, which allows user-assisted remote attackers to trigger access to an arbitrary URL via a crafted extension that is uninstalled.
CVE-2015-1299	Use-after-free vulnerability in the shared-timer implementation in Blink, as used in Google Chrome before 45.0.2454.85, allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging erroneous timer firing, related to ThreadTimers.cpp and Timer.cpp.
CVE-2015-1300	The FrameFetchContext::updateTimingInfoForIFrameNavigation function in core/loader/FrameFetchContext.cpp in Blink, as used in Google Chrome before 45.0.2454.85, does not properly restrict the availability of IFRAME Resource Timing API times, which allows remote attackers to obtain sensitive information via crafted JavaScript code that leverages a history.back call.
CVE-2015-1301	Multiple unspecified vulnerabilities in Google Chrome before 45.0.2454.85 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1302	The PDF viewer in Google Chrome before 46.0.2490.86 does not properly restrict scripting messages and API exposure, which allows remote attackers to bypass the Same Origin Policy via an unintended embedder or unintended plugin loading, related to pdf.js and out_of_process_instance.cc.
CVE-2015-1303	bindings/core/v8/V8DOMWrapper.h in Blink, as used in Google Chrome before 45.0.2454.101, does not perform a rethrow action to propagate information about a cross-context exception, which allows remote

	attackers to bypass the Same Origin Policy via a crafted HTML document containing an IFRAME element.
CVE-2015-1304	object-observe.js in Google V8, as used in Google Chrome before 45.0.2454.101, does not properly restrict method calls on access-checked objects, which allows remote attackers to bypass the Same Origin Policy via a (1) observe or (2) getNotifier call.
CVE-2015-1346	Multiple unspecified vulnerabilities in Google V8 before 3.30.33.15, as used in Google Chrome before 40.0.2214.91, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-1350	The VFS subsystem in the Linux kernel 3.x provides an incomplete set of requirements for setattr operations that underspecifies removing extended privilege attributes, which allows local users to cause a denial of service (capability stripping) via a failed invocation of a system call, as demonstrated by using chown to remove a capability from the ping or Wireshark dumpcap program.
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-2015-2059	The stringprep_utf8_to_ucs4 function in libin before 1.31, as used in jabberd2, allows context-dependent attackers to read system memory and possibly have

	other unspecified impact via invalid UTF-8 characters in a string, which triggers an out-of-bounds read.
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-2015-3218	The authentication_agent_new function in polkitbackend/polkitbackendinteractiveauthority.c in PolicyKit (aka polkit) before 0.113 allows local users to cause a denial of service (NULL pointer dereference and polkitd daemon crash) by calling RegisterAuthenticationAgent with an invalid object path.
CVE-2015-3255	The polkit_backend_action_pool_init function in polkitbackend/polkitbackendactionpool.c in PolicyKit (aka polkit) before 0.113 might allow local users to gain privileges via duplicate action IDs in action descriptions.
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-2015-3630	Docker Engine before 1.6.1 uses weak permissions for (1) /proc/asound, (2) /proc/timer_stats, (3) /proc/latency_stats, and (4) /proc/fs, which allows local users to modify the host, obtain sensitive information, and perform protocol downgrade attacks via a crafted image.
CVE-2015-3631	Docker Engine before 1.6.1 allows local users to set arbitrary Linux Security Modules (LSM) and docker_t policies via an image that allows volumes to override files in /proc.
CVE-2015-3885	Integer overflow in the ljpeg_start function in dcraw 7.00 and earlier allows remote attackers to cause a denial of service (crash) via a crafted image, which triggers a buffer overflow, related to the len variable.
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-2015-4625	Integer overflow in the authentication_agent_new_cookie function in PolicyKit (aka polkit) before 0.113 allows local users to gain privileges by creating a large number of connections, which triggers the issuance of a duplicate cookie value.
CVE-2015-4844	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.
CVE-2015-5116	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-2015-5180	res_query in libresolv in glibc before 2.25 allows remote attackers to cause a denial of service (NULL pointer dereference and process crash).
CVE-2015-5203	Double free vulnerability in the jasper_image_stop_load function in JasPer 1.900.17 allows remote attackers to cause a denial of service (crash) via a crafted JPEG 2000 image file.
CVE-2015-5221	Use-after-free vulnerability in the mif_process_cmpt function in libjasper/mif/mif_cod.c in the JasPer JPEG-2000 library before 1.900.2 allows remote attackers to cause a denial of service (crash) via a crafted JPEG 2000 image file.
CVE-2015-5370	Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not properly implement the DCE-RPC layer, which allows remote attackers to perform protocol-downgrade attacks, cause a denial of service (application crash or CPU consumption), or possibly execute arbitrary code on a client system via unspecified vectors.
CVE-2015-5377	** DISPUTED ** Elasticsearch before 1.6.1 allows remote attackers to execute arbitrary code via unspecified vectors involving the transport protocol. NOTE: ZDI appears to claim that CVE-2015-3253 and CVE-2015-5377 are the same vulnerability.
CVE-2015-5531	Directory traversal vulnerability in Elasticsearch before 1.6.1 allows remote attackers to read arbitrary files via unspecified vectors related to snapshot API calls.
CVE-2015-5539	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199

	allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5540	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5541	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5129.
CVE-2015-5544	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5545, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5552, and CVE-2015-5553.
CVE-2015-5545	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5544, CVE-2015-5546, CVE-2015-5547, CVE-2015-5548, CVE-2015-5549, CVE-2015-5552, and CVE-2015-5553.
CVE-2015-5546	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code

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

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

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

	CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5562	Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-5554, CVE-2015-5555, and CVE-2015-5558.
CVE-2015-5563	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5564	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, and CVE-2015-5565.
CVE-2015-5565	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before 18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, and CVE-2015-5564.
CVE-2015-5566	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.232 on Windows and OS X and before 11.2.202.508 on Linux, Adobe AIR before

	18.0.0.199, Adobe AIR SDK before 18.0.0.199, and Adobe AIR SDK & Compiler before 18.0.0.199 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5127, CVE-2015-5130, CVE-2015-5134, CVE-2015-5539, CVE-2015-5540, CVE-2015-5550, CVE-2015-5551, CVE-2015-5556, CVE-2015-5557, CVE-2015-5559, CVE-2015-5561, CVE-2015-5563, CVE-2015-5564, and CVE-2015-5565.
CVE-2015-5567	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5579.
CVE-2015-5568	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to cause a denial of service (vector-length corruption) or possibly have unspecified other impact via unknown vectors.
CVE-2015-5569	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 improperly implement the Flash broker API, which has unspecified impact and attack vectors.
CVE-2015-5570	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5574, CVE-2015-5581, CVE-2015-5584, and CVE-2015-6682.
CVE-2015-5571	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 do not properly restrict the SWF file format, which allows remote attackers to conduct cross-site request forgery (CSRF) attacks against JSONP endpoints, and obtain sensitive information, via a crafted OBJECT element with SWF content satisfying the character-set requirements of a

	callback API. NOTE: this issue exists because of an incomplete fix for CVE-2014-4671 and CVE-2014-5333.
CVE-2015-5572	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to bypass intended access restrictions and obtain sensitive information via unspecified vectors.
CVE-2015-5573	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion."
CVE-2015-5574	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5581, CVE-2015-5584, and CVE-2015-6682.
CVE-2015-5575	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.
CVE-2015-5576	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 do not properly restrict discovery of memory addresses, which allows attackers to bypass the ASLR protection mechanism via unspecified vectors.
CVE-2015-5577	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5578,

	CVE-2015-5580, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.
CVE-2015-5578	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5580, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.
CVE-2015-5579	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5567.
CVE-2015-5580	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5582, CVE-2015-5588, and CVE-2015-6677.
CVE-2015-5581	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5574, CVE-2015-5584, and CVE-2015-6682.
CVE-2015-5582	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5588, and CVE-2015-6677.
CVE-2015-5584	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on

	Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5574, CVE-2015-5581, and CVE-2015-6682.
CVE-2015-5587	Stack-based buffer overflow in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-5588	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, and CVE-2015-6677.
CVE-2015-5605	The regular-expression implementation in Google V8, as used in Google Chrome before 44.0.2403.89, mishandles interrupts, which allows remote attackers to cause a denial of service (application crash) via crafted JavaScript code, as demonstrated by an error in garbage collection during allocation of a stack-overflow exception message.
CVE-2015-5700	mktexlsr revision 22855 through revision 36625 as packaged in texlive allows local users to write to arbitrary files via a symlink attack.
CVE-2015-6580	Multiple unspecified vulnerabilities in Google V8 before 4.5.103.29, as used in Google Chrome before 45.0.2454.85, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-6581	Double free vulnerability in the opj_j2k_copy_default_tcp_and_create_tcd function in j2k.c in OpenJPEG before r3002, as used in PDFium in Google Chrome before 45.0.2454.85, allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by triggering a memory-allocation failure.
CVE-2015-6582	The decompose function in platform/transforms/TransformationMatrix.cpp in Blink, as used in Google Chrome before 45.0.2454.85, does not verify that a matrix inversion succeeded, which allows remote attackers to cause a denial of service (uninitialized

	memory access and application crash) or possibly have unspecified other impact via a crafted web site.
CVE-2015-6583	Google Chrome before 45.0.2454.85 does not display a location bar for a hosted app's window after navigation away from the installation site, which might make it easier for remote attackers to spoof content via a crafted app, related to browser.cc and hosted_app_browser_controller.cc.
CVE-2015-6676	Buffer overflow in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-6678.
CVE-2015-6677	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-5575, CVE-2015-5577, CVE-2015-5578, CVE-2015-5580, CVE-2015-5582, and CVE-2015-5588.
CVE-2015-6678	Buffer overflow in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-6676.
CVE-2015-6679	Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allow attackers to bypass the Same Origin Policy and obtain sensitive information via unspecified vectors.
CVE-2015-6682	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.241 and 19.x before 19.0.0.185 on Windows and OS X and before 11.2.202.521 on Linux, Adobe AIR before 19.0.0.190, Adobe AIR SDK before 19.0.0.190, and Adobe AIR SDK & Compiler before 19.0.0.190 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-5570, CVE-2015-5574, CVE-2015-5581, and CVE-2015-5584.

CVE-2015-6755	The ContainerNode::parserInsertBefore function in core/dom/ContainerNode.cpp in Blink, as used in Google Chrome before 46.0.2490.71, proceeds with a DOM tree insertion in certain cases where a parent node no longer contains a child node, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.
CVE-2015-6756	Use-after-free vulnerability in the CPDFSDK_PageView implementation in fpdfsdk/src/fsdk_mgr.cpp in PDFium, as used in Google Chrome before 46.0.2490.71, allows remote attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by leveraging mishandling of a focused annotation in a PDF document.
CVE-2015-6757	Use-after-free vulnerability in content/browser/service_worker/embedded_worker_instance.cc in the ServiceWorker implementation in Google Chrome before 46.0.2490.71 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging object destruction in a callback.
CVE-2015-6758	The CPDF_Document::GetPage function in fpdfapi/fpdf_parser/fpdf_parser_document.cpp in PDFium, as used in Google Chrome before 46.0.2490.71, does not properly perform a cast of a dictionary object, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document.
CVE-2015-6759	The shouldTreatAsUniqueOrigin function in platform/weborigin/SecurityOrigin.cpp in Blink, as used in Google Chrome before 46.0.2490.71, does not ensure that the origin of a LocalStorage resource is considered unique, which allows remote attackers to obtain sensitive information via vectors involving a blob: URL.
CVE-2015-6760	The Image11::map function in renderer/d3d/d3d11/Image11.cpp in libANGLE, as used in Google Chrome before 46.0.2490.71, mishandles mapping failures after device-lost events, which allows remote attackers to cause a denial of service (invalid read or write) or possibly have unspecified other impact via vectors involving a removed device.
CVE-2015-6761	The update_dimensions function in libavcodec/vp8.c in FFmpeg through 2.8.1, as used in Google Chrome before 46.0.2490.71 and other products, relies on a coefficient-partition count during multi-threaded operation, which allows remote attackers to cause a denial of service (race condition and memory corruption) or possibly have unspecified other impact via a crafted WebM file.
CVE-2015-6762	The CSSFontFaceSrcValue::fetch function in core/css/CSSFontFaceSrcValue.cpp in the Cascading Style

	Sheets (CSS) implementation in Blink, as used in Google Chrome before 46.0.2490.71, does not use the CORS cross-origin request algorithm when a font's URL appears to be a same-origin URL, which allows remote web servers to bypass the Same Origin Policy via a redirect.
CVE-2015-6763	Multiple unspecified vulnerabilities in Google Chrome before 46.0.2490.71 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-6764	The BasicJsonStringifier::SerializeJSArray function in json-stringifier.h in the JSON stringifier in Google V8, as used in Google Chrome before 47.0.2526.73, improperly loads array elements, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2015-6765	Use-after-free vulnerability in content/browser/appcache/appcache_update_job.cc in Google Chrome before 47.0.2526.73 allows remote attackers to execute arbitrary code or cause a denial of service by leveraging the mishandling of AppCache update jobs.
CVE-2015-6766	Use-after-free vulnerability in the AppCache implementation in Google Chrome before 47.0.2526.73 allows remote attackers with renderer access to cause a denial of service or possibly have unspecified other impact by leveraging incorrect AppCacheUpdateJob behavior associated with duplicate cache selection.
CVE-2015-6767	Use-after-free vulnerability in content/browser/appcache/appcache_dispatcher_host.cc in the AppCache implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact by leveraging incorrect pointer maintenance associated with certain callbacks.
CVE-2015-6768	The DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-6770.
CVE-2015-6769	The provisional-load commit implementation in WebKit/Source/bindings/core/v8/WindowProxy.cpp in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy by leveraging a delay in window proxy clearing.
CVE-2015-6770	The DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to bypass the Same Origin Policy via unspecified vectors, a different vulnerability than CVE-2015-6768.
CVE-2015-6771	js/array.js in Google V8, as used in Google Chrome before 47.0.2526.73, improperly implements certain

	map and filter operations for arrays, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted JavaScript code.
CVE-2015-6772	The DOM implementation in Blink, as used in Google Chrome before 47.0.2526.73, does not prevent javascript: URL navigation while a document is being detached, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code that improperly interacts with a plugin.
CVE-2015-6773	The convolution implementation in Skia, as used in Google Chrome before 47.0.2526.73, does not properly constrain row lengths, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via crafted graphics data.
CVE-2015-6774	Use-after-free vulnerability in the GetLoadTimes function in renderer/loadtimes_extension_bindings.cc in the Extensions implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that modifies a pointer used for reporting loadTimes data.
CVE-2015-6775	fpdfsdk/src/jsapi/fxjs_v8.cpp in PDFium, as used in Google Chrome before 47.0.2526.73, does not use signatures, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2015-6776	The opj_dwt_decode_1* functions in dwt.c in OpenJPEG, as used in PDFium in Google Chrome before 47.0.2526.73, allow remote attackers to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact via crafted JPEG 2000 data that is mishandled during a discrete wavelet transform.
CVE-2015-6777	Use-after-free vulnerability in the ContainerNode::notifyNodeInsertedInternal function in WebKit/Source/core/dom/ContainerNode.cpp in the DOM implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to DOMCharacterDataModified events for certain detached-subtree insertions.
CVE-2015-6778	The CJBig2_SymbolDict class in fxcodec/jbig2/JBig2_SymbolDict.cpp in PDFium, as used in Google Chrome before 47.0.2526.73, allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via a PDF document containing crafted data with JBIG2 compression.

CVE-2015-6779	PDFium, as used in Google Chrome before 47.0.2526.73, does not properly restrict use of chrome: URLs, which allows remote attackers to bypass intended scheme restrictions via a crafted PDF document, as demonstrated by a document with a link to a chrome://settings URL.
CVE-2015-6780	Use-after-free vulnerability in the Infobars implementation in Google Chrome before 47.0.2526.73 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted web site, related to browser/ui/views/website_settings/website_settings_popup_view.cc.
CVE-2015-6781	Integer overflow in the FontData::Bound function in data/font_data.cc in Google sfntly, as used in Google Chrome before 47.0.2526.73, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted offset or length value within font data in an SFNT container.
CVE-2015-6782	The Document::open function in WebKit/Source/core/dom/Document.cpp in Google Chrome before 47.0.2526.73 does not ensure that page-dismissal event handling is compatible with modal-dialog blocking, which makes it easier for remote attackers to spoof Omnibox content via a crafted web site.
CVE-2015-6784	The page serializer in Google Chrome before 47.0.2526.73 mishandles Mark of the Web (MOTW) comments for URLs containing a "--" sequence, which might allow remote attackers to inject HTML via a crafted URL, as demonstrated by an initial http://example.com?-- substring.
CVE-2015-6785	The CSPSource::hostMatches function in WebKit/Source/core/frame/csp/CSPSource.cpp in the Content Security Policy (CSP) implementation in Google Chrome before 47.0.2526.73 accepts an x.y hostname as a match for a *.x.y pattern, which might allow remote attackers to bypass intended access restrictions in opportunistic circumstances by leveraging a policy that was intended to be specific to subdomains.
CVE-2015-6786	The CSPSourceList::matches function in WebKit/Source/core/frame/csp/CSPSourceList.cpp in the Content Security Policy (CSP) implementation in Google Chrome before 47.0.2526.73 accepts a blob:, data:, or filesystem: URL as a match for a * pattern, which allows remote attackers to bypass intended scheme restrictions in opportunistic circumstances by leveraging a policy that relies on this pattern.
CVE-2015-6787	Multiple unspecified vulnerabilities in Google Chrome before 47.0.2526.73 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.

CVE-2015-6788	The ObjectBackedNativeHandler class in extensions/renderer/object_backed_native_handler.cc in the extensions subsystem in Google Chrome before 47.0.2526.80 improperly implements handler functions, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors that leverage "type confusion."
CVE-2015-6789	Race condition in the MutationObserver implementation in Blink, as used in Google Chrome before 47.0.2526.80, allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact by leveraging unanticipated object deletion.
CVE-2015-6790	The WebPageSerializerImpl::openTagToString function in WebKit/Source/web/WebPageSerializerImpl.cpp in the page serializer in Google Chrome before 47.0.2526.80 does not properly use HTML entities, which might allow remote attackers to inject arbitrary web script or HTML via a crafted document, as demonstrated by a double-quote character inside a single-quoted string.
CVE-2015-6791	Multiple unspecified vulnerabilities in Google Chrome before 47.0.2526.80 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-6792	The MIDI subsystem in Google Chrome before 47.0.2526.106 does not properly handle the sending of data, which allows remote attackers to execute arbitrary code or cause a denial of service (application crash) via unspecified vectors, related to midi_manager.cc, midi_manager_alsa.cc, and midi_manager_mac.cc, a different vulnerability than CVE-2015-8664.
CVE-2015-7552	Heap-based buffer overflow in the gdk_pixbuf_flip function in gdk-pixbuf-scale.c in gdk-pixbuf 2.30.x allows remote attackers to cause a denial of service or possibly execute arbitrary code via a crafted BMP file.
CVE-2015-7554	The _TIFFVGetField function in tif_dir.c in libtiff 4.0.6 allows attackers to cause a denial of service (invalid memory write and crash) or possibly have unspecified other impact via crafted field data in an extension tag in a TIFF image.
CVE-2015-7625	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7626,

	CVE-2015-7627, CVE-2015-7630, CVE-2015-7633, and CVE-2015-7634.
CVE-2015-7626	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7627, CVE-2015-7630, CVE-2015-7633, and CVE-2015-7634.
CVE-2015-7627	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7626, CVE-2015-7630, CVE-2015-7633, and CVE-2015-7634.
CVE-2015-7628	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow remote attackers to bypass the Same Origin Policy and obtain sensitive information via unspecified vectors.
CVE-2015-7629	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via a TextFormat object with a crafted tabStops property, a different vulnerability than CVE-2015-7631, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7630	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7633, and CVE-2015-7634.
CVE-2015-7631	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on

	Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via a TextLine object with a crafted validity property, a different vulnerability than CVE-2015-7629, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7632	Buffer overflow in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via a Loader object with a crafted loaderBytes property.
CVE-2015-7633	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7630, and CVE-2015-7634.
CVE-2015-7634	Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-7625, CVE-2015-7626, CVE-2015-7627, CVE-2015-7630, and CVE-2015-7633.
CVE-2015-7635	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7636	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than

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

	Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7642, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7642	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, CVE-2015-7635, CVE-2015-7636, CVE-2015-7637, CVE-2015-7638, CVE-2015-7639, CVE-2015-7640, CVE-2015-7641, CVE-2015-7643, and CVE-2015-7644.
CVE-2015-7643	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via a Video object with a crafted deblocking property, a different vulnerability than CVE-2015-7629, CVE-2015-7631, and CVE-2015-7644.
CVE-2015-7644	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.252 and 19.x before 19.0.0.207 on Windows and OS X and before 11.2.202.535 on Linux, Adobe AIR before 19.0.0.213, Adobe AIR SDK before 19.0.0.213, and Adobe AIR SDK & Compiler before 19.0.0.213 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7629, CVE-2015-7631, and CVE-2015-7643.
CVE-2015-7645	Adobe Flash Player 18.x through 18.0.0.252 and 19.x through 19.0.0.207 on Windows and OS X and 11.x through 11.2.202.535 on Linux allows remote attackers to execute arbitrary code via a crafted SWF file, as exploited in the wild in October 2015.
CVE-2015-7647	Adobe Flash Player before 18.0.0.255 and 19.x before 19.0.0.226 on Windows and OS X and before 11.2.202.540 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-7648.
CVE-2015-7648	Adobe Flash Player before 18.0.0.255 and 19.x before 19.0.0.226 on Windows and OS X and before 11.2.202.540 on Linux allows attackers to

	execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-7647.
CVE-2015-7651	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted DefineFunction atoms, a different vulnerability than CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7652	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via a crafted gridFitType property value, a different vulnerability than CVE-2015-7651, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7653	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted globalToLocal arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7654	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted attachSound arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658,

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

	CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7659	Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion" in the NetConnection object implementation.
CVE-2015-7660	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via crafted setMask arguments, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7661	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via a crafted getBounds call, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7662	Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allow remote attackers to bypass intended access restrictions and write to files via unspecified vectors.
CVE-2015-7663	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.261 and 19.x before 19.0.0.245 on Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than

	CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-8042, CVE-2015-8043, CVE-2015-8044, and CVE-2015-8046.
CVE-2015-7834	Multiple unspecified vulnerabilities in Google V8 before 4.6.85.23, as used in Google Chrome before 46.0.2490.71, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-7837	The Linux kernel, as used in Red Hat Enterprise Linux 7, kernel-rt, and Enterprise MRG 2 and when booted with UEFI Secure Boot enabled, allows local users to bypass intended securelevel/secureboot restrictions by leveraging improper handling of secure_boot flag across kexec reboot.
CVE-2015-7973	NTP before 4.2.8p6 and 4.3.x before 4.3.90, when configured in broadcast mode, allows man-in-the-middle attackers to conduct replay attacks by sniffing the network.
CVE-2015-7974	NTP 4.x before 4.2.8p6 and 4.3.x before 4.3.90 do not verify peer associations of symmetric keys when authenticating packets, which might allow remote attackers to conduct impersonation attacks via an arbitrary trusted key, aka a "skeleton key."
CVE-2015-7975	The nextvar function in NTP before 4.2.8p6 and 4.3.x before 4.3.90 does not properly validate the length of its input, which allows an attacker to cause a denial of service (application crash).
CVE-2015-7976	The ntpq saveconfig command in NTP 4.1.2, 4.2.x before 4.2.8p6, 4.3, 4.3.25, 4.3.70, and 4.3.77 does not properly filter special characters, which allows attackers to cause unspecified impact via a crafted filename.
CVE-2015-7977	ntpd in NTP before 4.2.8p6 and 4.3.x before 4.3.90 allows remote attackers to cause a denial of service (NULL pointer dereference) via a ntpdc reslist command.
CVE-2015-7978	NTP before 4.2.8p6 and 4.3.0 before 4.3.90 allows a remote attackers to cause a denial of service (stack exhaustion) via an ntpdc relist command, which triggers recursive traversal of the restriction list.
CVE-2015-7979	NTP before 4.2.8p6 and 4.3.x before 4.3.90 allows remote attackers to cause a denial of service (client-server association tear down) by sending broadcast packets with invalid authentication to a broadcast client.
CVE-2015-7995	The xsltStylePreCompute function in preproc.c in libxslt 1.1.28 does not check if the parent node is an element, which allows attackers to cause a denial of service via a crafted XML file, related to a "type confusion" issue.

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

	Windows and OS X and before 11.2.202.548 on Linux, Adobe AIR before 19.0.0.241, Adobe AIR SDK before 19.0.0.241, and Adobe AIR SDK & Compiler before 19.0.0.241 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-7651, CVE-2015-7652, CVE-2015-7653, CVE-2015-7654, CVE-2015-7655, CVE-2015-7656, CVE-2015-7657, CVE-2015-7658, CVE-2015-7660, CVE-2015-7661, CVE-2015-7663, CVE-2015-8042, CVE-2015-8043, and CVE-2015-8044.
CVE-2015-8047	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8048	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8049	Use-after-free vulnerability in the TextField object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on

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

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

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

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

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

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

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

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

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

	CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8126	Multiple buffer overflows in the (1) png_set_PLTE and (2) png_get_PLTE functions in libpng before 1.0.64, 1.1.x and 1.2.x before 1.2.54, 1.3.x and 1.4.x before 1.4.17, 1.5.x before 1.5.24, and 1.6.x before 1.6.19 allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a small bit-depth value in an IHDR (aka image header) chunk in a PNG image.
CVE-2015-8138	NTP before 4.2.8p6 and 4.3.x before 4.3.90 allows remote attackers to bypass the origin timestamp validation via a packet with an origin timestamp set to zero.
CVE-2015-8158	The getresponse function in ntpq in NTP versions before 4.2.8p9 and 4.3.x before 4.3.90 allows remote attackers to cause a denial of service (infinite loop) via crafted packets with incorrect values.
CVE-2015-8270	The AMF3ReadString function in amf.c in RTMPDump 2.4 allows remote RTMP Media servers to cause a denial of service (invalid pointer dereference and process crash).
CVE-2015-8271	The AMF3CD_AddProp function in amf.c in RTMPDump 2.4 allows remote RTMP Media servers to execute arbitrary code.
CVE-2015-8272	RTMPDump 2.4 allows remote attackers to trigger a denial of service (NULL pointer dereference and process crash).
CVE-2015-8366	** 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-2015-8367	** 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-2015-8401	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR

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

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

	SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8406	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8407	Stack-based buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK

	before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8457.
CVE-2015-8408	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8409	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2015-8440 and CVE-2015-8453.
CVE-2015-8410	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8411	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228

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

	on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8414	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8415	Buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on

	Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-8416	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8417	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8418	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8419	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418,

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

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

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

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

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

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

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

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

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

	CVE-2015-8435, CVE-2015-8436, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8438	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a crafted XML object that is mishandled during a toString call, a different vulnerability than CVE-2015-8446.
CVE-2015-8439	The SharedObject object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code by leveraging an unspecified "type confusion" during a getRemote call, a different vulnerability than CVE-2015-8456.
CVE-2015-8440	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to bypass intended access restrictions via unspecified vectors, a different vulnerability than CVE-2015-8409 and CVE-2015-8453.
CVE-2015-8441	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433,

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

	CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8451, and CVE-2015-8455.
CVE-2015-8445	Integer overflow in the Shader filter implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via a large BitmapData source object.
CVE-2015-8446	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via an MP3 file with COMM tags that are mishandled during memory allocation, a different vulnerability than CVE-2015-8438.
CVE-2015-8447	Use-after-free vulnerability in the Color object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted setTransform arguments, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, and CVE-2015-8454.
CVE-2015-8448	Use-after-free vulnerability in the DisplacementMapFilter object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before

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

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

	CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, and CVE-2015-8454.
CVE-2015-8453	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to bypass the ASLR protection mechanism via JIT data, a different vulnerability than CVE-2015-8409 and CVE-2015-8440.
CVE-2015-8454	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, and CVE-2015-8452.
CVE-2015-8455	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified

	vectors, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, and CVE-2015-8451.
CVE-2015-8456	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2015-8439.
CVE-2015-8457	Stack-based buffer overflow in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8407.
CVE-2015-8459	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8460, CVE-2015-8636, and CVE-2015-8645.
CVE-2015-8460	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8459, CVE-2015-8636, and CVE-2015-8645.
CVE-2015-8478	Multiple unspecified vulnerabilities in Google V8 before 4.7.80.23, as used in Google Chrome before 47.0.2526.73, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2015-8479	Use-after-free vulnerability in the AudioOutputDevice::OnDeviceAuthorized function in media/audio/audio_output_device.cc in Google Chrome before 47.0.2526.73 allows attackers to cause a denial of service (heap memory corruption) or possibly have unspecified other impact by triggering access to an unauthorized audio output device.

CVE-2015-8480	The VideoFramePool::PoolImpl::CreateFrame function in media/base/video_frame_pool.cc in Google Chrome before 47.0.2526.73 does not initialize memory for a video-frame data structure, which might allow remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact by leveraging improper interaction with the vp3_h_loop_filter_c function in libavcodec/vp3dsp.c in FFmpeg.
CVE-2015-8548	Multiple unspecified vulnerabilities in Google V8 before 4.7.80.23, as used in Google Chrome before 47.0.2526.80, allow attackers to cause a denial of service or possibly have other impact via unknown vectors, a different issue than CVE-2015-8478.
CVE-2015-8634	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.
CVE-2015-8635	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.
CVE-2015-8636	Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2015-8459, CVE-2015-8460, and CVE-2015-8645.
CVE-2015-8638	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR

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

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

	vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8648, CVE-2015-8649, and CVE-2015-8650.
CVE-2015-8648	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8649, and CVE-2015-8650.
CVE-2015-8649	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, and CVE-2015-8650.
CVE-2015-8650	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2015-8634, CVE-2015-8635, CVE-2015-8638, CVE-2015-8639, CVE-2015-8640, CVE-2015-8641, CVE-2015-8642, CVE-2015-8643, CVE-2015-8646, CVE-2015-8647, CVE-2015-8648, and CVE-2015-8649.
CVE-2015-8651	Integer overflow in Adobe Flash Player before 18.0.0.324 and 19.x and 20.x before 20.0.0.267 on Windows and OS X and before 11.2.202.559 on Linux, Adobe AIR before 20.0.0.233, Adobe AIR SDK before 20.0.0.233, and Adobe AIR SDK & Compiler before 20.0.0.233 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2015-8652	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before

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

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

	CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, CVE-2015-8455, CVE-2015-8652, CVE-2015-8654, CVE-2015-8656, CVE-2015-8658, and CVE-2015-8820.
CVE-2015-8658	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (uninitialized pointer dereference and memory corruption) via crafted MPEG-4 data, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, CVE-2015-8455, CVE-2015-8652, CVE-2015-8654, CVE-2015-8656, CVE-2015-8657, and CVE-2015-8820.
CVE-2015-8664	Integer overflow in the WebCursor::Deserialize function in content/common/cursors/webcursor.cc in Google Chrome before 47.0.2526.106 allows remote attackers to cause a denial of service or possibly have unspecified other impact via an RGBA pixel array with crafted dimensions, a different vulnerability than CVE-2015-6792.
CVE-2015-8668	Heap-based buffer overflow in the PackBitsPreEncode function in tif_packbits.c in bmp2tiff in libtiff 4.0.6 and earlier allows remote attackers to execute arbitrary code or cause a denial of service via a large width field in a BMP image.
CVE-2015-8806	dict.c in libxml2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via an unexpected character immediately after the "<!DOCTYPE html" substring in a crafted HTML document.
CVE-2015-8820	Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allow attackers to execute arbitrary code or cause a denial of service (out-of-bounds read and memory corruption) via crafted MPEG-4 data, a different vulnerability than CVE-2015-8045, CVE-2015-8047, CVE-2015-8060, CVE-2015-8408, CVE-2015-8416, CVE-2015-8417, CVE-2015-8418, CVE-2015-8419, CVE-2015-8443, CVE-2015-8444, CVE-2015-8451, CVE-2015-8455,

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

	CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, CVE-2015-8454, CVE-2015-8653, CVE-2015-8655, and CVE-2015-8821.
CVE-2015-8823	Use-after-free vulnerability in the TextField object implementation in Adobe Flash Player before 18.0.0.268 and 19.x and 20.x before 20.0.0.228 on Windows and OS X and before 11.2.202.554 on Linux, Adobe AIR before 20.0.0.204, Adobe AIR SDK before 20.0.0.204, and Adobe AIR SDK & Compiler before 20.0.0.204 allows attackers to execute arbitrary code via crafted text property, a different vulnerability than CVE-2015-8048, CVE-2015-8049, CVE-2015-8050, CVE-2015-8055, CVE-2015-8056, CVE-2015-8057, CVE-2015-8058, CVE-2015-8059, CVE-2015-8061, CVE-2015-8062, CVE-2015-8063, CVE-2015-8064, CVE-2015-8065, CVE-2015-8066, CVE-2015-8067, CVE-2015-8068, CVE-2015-8069, CVE-2015-8070, CVE-2015-8071, CVE-2015-8401, CVE-2015-8402, CVE-2015-8403, CVE-2015-8404, CVE-2015-8405, CVE-2015-8406, CVE-2015-8410, CVE-2015-8411, CVE-2015-8412, CVE-2015-8413, CVE-2015-8414, CVE-2015-8420, CVE-2015-8421, CVE-2015-8422, CVE-2015-8423, CVE-2015-8424, CVE-2015-8425, CVE-2015-8426, CVE-2015-8427, CVE-2015-8428, CVE-2015-8429, CVE-2015-8430, CVE-2015-8431, CVE-2015-8432, CVE-2015-8433, CVE-2015-8434, CVE-2015-8435, CVE-2015-8436, CVE-2015-8437, CVE-2015-8441, CVE-2015-8442, CVE-2015-8447, CVE-2015-8448, CVE-2015-8449, CVE-2015-8450, CVE-2015-8452, CVE-2015-8454, CVE-2015-8653, CVE-2015-8655, CVE-2015-8821, and CVE-2015-8822.
CVE-2015-8839	Multiple race conditions in the ext4 filesystem implementation in the Linux kernel before 4.5 allow local users to cause a denial of service (disk corruption) by writing to a page that is associated with a different user's file after unsynchronized hole punching and page-fault handling.
CVE-2015-8853	The (1) S_reghop3, (2) S_reghop4, and (3) S_reghopmaybe3 functions in regexec.c in Perl before 5.24.0 allow context-dependent attackers to cause a denial of service (infinite loop) via crafted utf-8 data, as demonstrated by "a\x80."
CVE-2015-8865	The file_check_mem function in funcs.c in file before 5.23, as used in the Fileinfo component in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5, mishandles continuation-level jumps, which allows context-dependent attackers to cause a denial of

	service (buffer overflow and application crash) or possibly execute arbitrary code via a crafted magic file.
CVE-2015-8872	The set_fat function in fat.c in dosfstools before 4.0 might allow attackers to corrupt a FAT12 filesystem or cause a denial of service (invalid memory read and crash) by writing an odd number of clusters to the third to last entry on a FAT12 filesystem, which triggers an "off-by-two error."
CVE-2015-8874	Stack consumption vulnerability in GD in PHP before 5.6.12 allows remote attackers to cause a denial of service via a crafted imagefilltoborder call.
CVE-2015-8875	Multiple integer overflows in the (1) pixops_composite_nearest, (2) pixops_composite_color_nearest, and (3) pixops_process functions in pixops/pixops.c in gdk-pixbuf before 2.33.1 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted image, which triggers a heap-based buffer overflow.
CVE-2015-8877	The gdImageScaleTwoPass function in gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.2.0, as used in PHP before 5.6.12, uses inconsistent allocate and free approaches, which allows remote attackers to cause a denial of service (memory consumption) via a crafted call, as demonstrated by a call to the PHP imagescale function.
CVE-2015-8899	Dnsmasq before 2.76 allows remote servers to cause a denial of service (crash) via a reply with an empty DNS address that has an (1) A or (2) AAAA record defined locally.
CVE-2015-8916	bsdtar in libarchive before 3.2.0 returns a success code without filling the entry when the header is a "split file in multivolume RAR," which allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted rar file.
CVE-2015-8917	bsdtar in libarchive before 3.2.0 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via an invalid character in the name of a cab file.
CVE-2015-8919	The lha_read_file_extended_header function in archive_read_support_format_lha.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds heap) via a crafted (1) lzh or (2) lha file.
CVE-2015-8920	The _ar_read_header function in archive_read_support_format_ar.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds stack read) via a crafted ar file.

CVE-2015-8921	The ae_strtofflags function in archive_entry.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mtree file.
CVE-2015-8922	The read_CodersInfo function in archive_read_support_format_7zip.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted 7z file, related to the _7z_folder struct.
CVE-2015-8923	The process_extra function in libarchive before 3.2.0 uses the size field and a signed number in an offset, which allows remote attackers to cause a denial of service (crash) via a crafted zip file.
CVE-2015-8924	The archive_read_format_tar_read_header function in archive_read_support_format_tar.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted tar file.
CVE-2015-8925	The readline function in archive_read_support_format_mtree.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (invalid read) via a crafted mtree file, related to newline parsing.
CVE-2015-8926	The archive_read_format_rar_read_data function in archive_read_support_format_rar.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (crash) via a crafted rar archive.
CVE-2015-8928	The process_add_entry function in archive_read_support_format_mtree.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mtree file.
CVE-2015-8930	bsdtar in libarchive before 3.2.0 allows remote attackers to cause a denial of service (infinite loop) via an ISO with a directory that is a member of itself.
CVE-2015-8931	Multiple integer overflows in the (1) get_time_t_max and (2) get_time_t_min functions in archive_read_support_format_mtree.c in libarchive before 3.2.0 allow remote attackers to have unspecified impact via a crafted mtree file, which triggers undefined behavior.
CVE-2015-8932	The compress_bidder_init function in archive_read_support_filter_compress.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (crash) via a crafted tar file, which triggers an invalid left shift.
CVE-2015-8933	Integer overflow in the archive_read_format_tar_skip function in archive_read_support_format_tar.c in libarchive before 3.2.0 allows remote attackers to cause a denial of service (crash) via a crafted tar file.

CVE-2015-8934	The copy_from_lzss_window function in archive_read_support_format_rar.c in libarchive 3.2.0 and earlier allows remote attackers to cause a denial of service (out-of-bounds heap read) via a crafted rar file.
CVE-2015-8944	The ioresources_init function in kernel/resource.c in the Linux kernel through 4.7, as used in Android before 2016-08-05 on Nexus 6 and 7 (2013) devices, uses weak permissions for /proc/iomem, which allows local users to obtain sensitive information by reading this file, aka Android internal bug 28814213 and Qualcomm internal bug CR786116. NOTE: the permissions may be intentional in most non-Android contexts.
CVE-2015-8947	hb-ot-layout-gpos-table.hh in HarfBuzz before 1.0.5 allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via crafted data, a different vulnerability than CVE-2016-2052.
CVE-2015-8948	idn in GNU libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a zero byte as input, which triggers an out-of-bounds read.
CVE-2015-8952	The mbcache feature in the ext2 and ext4 filesystem implementations in the Linux kernel before 4.6 mishandles xattr block caching, which allows local users to cause a denial of service (soft lockup) via filesystem operations in environments that use many attributes, as demonstrated by Ceph and Samba.
CVE-2015-8964	The tty_set_termios_ldisc function in drivers/tty/tty_ldisc.c in the Linux kernel before 4.5 allows local users to obtain sensitive information from kernel memory by reading a tty data structure.
CVE-2015-8982	Integer overflow in the strxfrm function in the GNU C Library (aka glibc or libc6) before 2.21 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string, which triggers a stack-based buffer overflow.
CVE-2015-8983	Integer overflow in the _IO_wstr_overflow function in libio/wstrops.c in the GNU C Library (aka glibc or libc6) before 2.22 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors related to computing a size in bytes, which triggers a heap-based buffer overflow.
CVE-2015-8984	The fnmatch function in the GNU C Library (aka glibc or libc6) before 2.22 might allow context-dependent attackers to cause a denial of service (application crash) via a malformed pattern, which triggers an out-of-bounds read.
CVE-2015-9096	Net::SMTP in Ruby before 2.4.0 is vulnerable to SMTP command injection via CRLF sequences in a RCPT

	TO or MAIL FROM command, as demonstrated by CRLF sequences immediately before and after a DATA substring.
CVE-2015-9252	An issue was discovered in QPDF before 7.0.0. Endless recursion causes stack exhaustion in QPDFTokenizer::resolveLiteral() in QPDFTokenizer.cc, related to the QPDF::resolve function in QPDF.cc.
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-2016-0494	Unspecified vulnerability in the Java SE and Java SE Embedded components in Oracle Java SE 6u105, 7u91, and 8u66 and Java SE Embedded 8u65 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.
CVE-2016-0634	The expansion of '\h' in the prompt string in bash 4.3 allows remote authenticated users to execute arbitrary code via shell metacharacters placed in 'hostname' of a machine.
CVE-2016-0639	Unspecified vulnerability in Oracle MySQL 5.6.29 and earlier and 5.7.11 and earlier allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Pluggable Authentication.
CVE-2016-0642	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier allows local users to affect integrity and availability via vectors related to Federated.
CVE-2016-0643	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows local users to affect confidentiality via vectors related to DML.
CVE-2016-0647	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows local users to affect availability via vectors related to FTS.
CVE-2016-0648	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows local users to affect availability via vectors related to PS.
CVE-2016-0655	Unspecified vulnerability in Oracle MySQL 5.6.29 and earlier and 5.7.11 and earlier and MariaDB 10.0.x before 10.0.25 and 10.1.x before 10.1.14 allows local users to affect availability via vectors related to InnoDB.

CVE-2016-0657	Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect confidentiality via vectors related to JSON.
CVE-2016-0659	Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect availability via vectors related to Optimizer.
CVE-2016-0662	Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect availability via vectors related to Partition.
CVE-2016-0666	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows local users to affect availability via vectors related to Security: Privileges.
CVE-2016-0667	Unspecified vulnerability in Oracle MySQL 5.7.11 and earlier allows local users to affect availability via vectors related to Locking.
CVE-2016-0686	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77 and Java SE Embedded 8u77 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Serialization.
CVE-2016-0687	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77 and Java SE Embedded 8u77 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to the Hotspot sub-component.
CVE-2016-0695	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77; Java SE Embedded 8u77; and JRockit R28.3.9 allows remote attackers to affect confidentiality via vectors related to Security.
CVE-2016-0718	Expat allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a malformed input document, which triggers a buffer overflow.
CVE-2016-0727	The crontab script in the ntp package before 1:4.2.6.p3+dfsg-1ubuntu3.11 on Ubuntu 12.04 LTS, before 1:4.2.6.p5+dfsg-3ubuntu2.14.04.10 on Ubuntu 14.04 LTS, on Ubuntu Wily, and before 1:4.2.8p4+dfsg-3ubuntu5.3 on Ubuntu 16.04 LTS allows local users with access to the ntp account to write to arbitrary files and consequently gain privileges via vectors involving statistics directory cleanup.
CVE-2016-0736	In Apache HTTP Server versions 2.4.0 to 2.4.23, mod_session_crypto was encrypting its data/cookie using the configured ciphers with possibly either CBC or ECB modes of operation (AES256-CBC by default), hence no selectable or builtin authenticated encryption. This made it vulnerable to padding oracle attacks, particularly with CBC.

CVE-2016-0749	The smartcard interaction in SPICE allows remote attackers to cause a denial of service (QEMU-KVM process crash) or possibly execute arbitrary code via vectors related to connecting to a guest VM, which triggers a heap-based buffer overflow.
CVE-2016-0758	Integer overflow in lib/asn1_decoder.c in the Linux kernel before 4.6 allows local users to gain privileges via crafted ASN.1 data.
CVE-2016-0762	The Realm implementations in Apache Tomcat versions 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 did not process the supplied password if the supplied user name did not exist. This made a timing attack possible to determine valid user names. Note that the default configuration includes the LockOutRealm which makes exploitation of this vulnerability harder.
CVE-2016-0772	The smtplib library in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 does not return an error when StartTLS fails, which might allow man-in-the-middle attackers to bypass the TLS protections by leveraging a network position between the client and the registry to block the StartTLS command, aka a "StartTLS stripping attack."
CVE-2016-0959	Use after free vulnerability in Adobe Flash Player Desktop Runtime before 20.0.0.267, Adobe Flash Player Extended Support Release before 18.0.0.324, Adobe Flash Player for Google Chrome before 20.0.0.267, Adobe Flash Player for Microsoft Edge and Internet Explorer 11 before 20.0.0.267, Adobe Flash Player for Internet Explorer 10 and 11 before 20.0.0.267, Adobe Flash Player for Linux before 11.2.202.559, AIR Desktop Runtime before 20.0.0.233, AIR SDK before 20.0.0.233, AIR SDK & Compiler before 20.0.0.233, AIR for Android before 20.0.0.233.
CVE-2016-0960	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0961, CVE-2016-0962, CVE-2016-0986, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.
CVE-2016-0961	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code

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

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

CVE-2016-0970	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0972, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.
CVE-2016-0971	Heap-based buffer overflow in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors.
CVE-2016-0972	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0964, CVE-2016-0965, CVE-2016-0966, CVE-2016-0967, CVE-2016-0968, CVE-2016-0969, CVE-2016-0970, CVE-2016-0976, CVE-2016-0977, CVE-2016-0978, CVE-2016-0979, CVE-2016-0980, and CVE-2016-0981.
CVE-2016-0973	Use-after-free vulnerability in the URLRequest object implementation in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via a URLLoader.load call, a different vulnerability than CVE-2016-0974, CVE-2016-0975, CVE-2016-0982, CVE-2016-0983, and CVE-2016-0984.
CVE-2016-0974	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0973,

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

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

CVE-2016-0983	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0973, CVE-2016-0974, CVE-2016-0975, CVE-2016-0982, and CVE-2016-0984.
CVE-2016-0984	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0973, CVE-2016-0974, CVE-2016-0975, CVE-2016-0982, and CVE-2016-0983.
CVE-2016-0985	Adobe Flash Player before 18.0.0.329 and 19.x and 20.x before 20.0.0.306 on Windows and OS X and before 11.2.202.569 on Linux, Adobe AIR before 20.0.0.260, Adobe AIR SDK before 20.0.0.260, and Adobe AIR SDK & Compiler before 20.0.0.260 allow attackers to execute arbitrary code by leveraging an unspecified "type confusion."
CVE-2016-0986	Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-0960, CVE-2016-0961, CVE-2016-0962, CVE-2016-0989, CVE-2016-0992, CVE-2016-1002, and CVE-2016-1005.
CVE-2016-0987	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.

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

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

CVE-2016-0997	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0998, CVE-2016-0999, and CVE-2016-1000.
CVE-2016-0998	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0999, and CVE-2016-1000.
CVE-2016-0999	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, and CVE-2016-1000.
CVE-2016-1000	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.333 and 19.x through 21.x before 21.0.0.182 on Windows and OS X and before 11.2.202.577 on Linux, Adobe AIR before 21.0.0.176, Adobe AIR SDK before 21.0.0.176, and Adobe AIR SDK & Compiler before 21.0.0.176 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-0987, CVE-2016-0988, CVE-2016-0990, CVE-2016-0991, CVE-2016-0994, CVE-2016-0995, CVE-2016-0996, CVE-2016-0997, CVE-2016-0998, and CVE-2016-0999.
CVE-2016-1000110	It was discovered that the Python CGIHandler class did not properly protect against the HTTP_PROXY variable name clash in a CGI context. A remote attacker

	could possibly use this flaw to redirect HTTP requests performed by a Python CGI script to an attacker-controlled proxy via a malicious HTTP request.
CVE-2016-1000111	It was discovered that python-twisted-web used the value of the Proxy header from HTTP requests to initialize the HTTP_PROXY environment variable for CGI scripts, which in turn was incorrectly used by certain HTTP client implementations to configure the proxy for outgoing HTTP requests. A remote attacker could possibly use this flaw to redirect HTTP requests performed by a CGI script to an attacker-controlled proxy via a malicious HTTP request.
CVE-2016-10002	Incorrect processing of responses to If-None-Modified HTTP conditional requests in Squid HTTP Proxy 3.1.10 through 3.1.23, 3.2.0.3 through 3.5.22, and 4.0.1 through 4.0.16 leads to client-specific Cookie data being leaked to other clients. Attack requests can easily be crafted by a client to probe a cache for this information.
CVE-2016-10003	Incorrect HTTP Request header comparison in Squid HTTP Proxy 3.5.0.1 through 3.5.22, and 4.0.1 through 4.0.16 results in Collapsed Forwarding feature mistakenly identifying some private responses as being suitable for delivery to multiple clients.
CVE-2016-10009	Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.
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-2016-10010	sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.
CVE-2016-10011	authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.
CVE-2016-10012	The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a

	sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.
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-2016-10028	The virgl_cmd_get_capset function in hw/display/virtio-gpu-3d.c in QEMU (aka Quick Emulator) built with Virtio GPU Device emulator support allows local guest OS users to cause a denial of service (out-of-bounds read and process crash) via a VIRTIO_GPU_CMD_GET_CAPSET command with a maximum capabilities size with a value of 0.
CVE-2016-10029	The virtio_gpu_set_scanout function in QEMU (aka Quick Emulator) built with Virtio GPU Device emulator support allows local guest OS users to cause a denial of service (out-of-bounds read and process crash) via a scanout id in a VIRTIO_GPU_CMD_SET_SCANOUT command larger than num_scanouts.
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-2016-10062	The ReadGROUP4Image function in coders/tiff.c in ImageMagick does not check the return value of the fwrite function, which allows remote attackers to cause a denial of service (application crash) via a crafted file.
CVE-2016-10087	The png_set_text_2 function in libpng 0.71 before 1.0.67, 1.2.x before 1.2.57, 1.4.x before 1.4.20, 1.5.x before 1.5.28, and 1.6.x before 1.6.27 allows context-dependent attackers to cause a NULL pointer dereference vectors involving loading a text chunk into

	a png structure, removing the text, and then adding another text chunk to the structure.
CVE-2016-10088	The sg implementation in the Linux kernel through 4.9 does not properly restrict write operations in situations where the KERNEL_DS option is set, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device, related to block/bsg.c and drivers/scsi/sg.c. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-9576.
CVE-2016-10092	Heap-based buffer overflow in the readContigStripsIntoBuffer function in tif_unix.c in LibTIFF 4.0.7 allows remote attackers to have unspecified impact via a crafted image.
CVE-2016-10093	Integer overflow in tools/tiffcp.c in LibTIFF 4.0.7 allows remote attackers to have unspecified impact via a crafted image, which triggers a heap-based buffer overflow.
CVE-2016-10094	Off-by-one error in the t2p_readwrite_pdf_image_tile function in tools/tiff2pdf.c in LibTIFF 4.0.7 allows remote attackers to have unspecified impact via a crafted image.
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-2016-10109	Use-after-free vulnerability in pcsc-lite before 1.8.20 allows a remote attackers to cause denial of service (crash) via a command that uses "cardsList" after the handle has been released through the SCardReleaseContext function.
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-2016-10144	coders/ipl.c in ImageMagick allows remote attackers to have unspecific impact by leveraging a missing malloc check.
CVE-2016-10145	Off-by-one error in coders/wpg.c in ImageMagick allows remote attackers to have unspecified impact via vectors related to a string copy.
CVE-2016-10146	Multiple memory leaks in the caption and label handling code in ImageMagick allow remote attackers to cause a denial of service (memory consumption) via unspecified vectors.
CVE-2016-10147	crypto/mcryptd.c in the Linux kernel before 4.8.15 allows local users to cause a denial of service (NULL pointer dereference and system crash) by using an AF_ALG socket with an incompatible algorithm, as demonstrated by mcryptd(md5).
CVE-2016-10149	XML External Entity (XXE) vulnerability in PySAML2 4.4.0 and earlier allows remote attackers to read arbitrary files via a crafted SAML XML request or response.
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-2016-10155	Memory leak in hw/watchdog/wdt_i6300esb.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption and QEMU process crash) via a large number of device unplug operations.
CVE-2016-10158	The exif_convert_any_to_int function in ext/exif/exif.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial

	of service (application crash) via crafted EXIF data that triggers an attempt to divide the minimum representable negative integer by -1.
CVE-2016-10159	Integer overflow in the phar_parse_pharfile function in ext/phar/phar.c in PHP before 5.6.30 and 7.0.x before 7.0.15 allows remote attackers to cause a denial of service (memory consumption or application crash) via a truncated manifest entry in a PHAR archive.
CVE-2016-1016	Use-after-free vulnerability in the Transform object implementation in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via a flash.geom.Matrix callback, a different vulnerability than CVE-2016-1011, CVE-2016-1013, CVE-2016-1017, and CVE-2016-1031.
CVE-2016-10160	Off-by-one error in the phar_parse_pharfile function in ext/phar/phar.c in PHP before 5.6.30 and 7.0.x before 7.0.15 allows remote attackers to cause a denial of service (memory corruption) or possibly execute arbitrary code via a crafted PHAR archive with an alias mismatch.
CVE-2016-10161	The object_common1 function in ext/standard/var_unserializer.c in PHP before 5.6.30, 7.0.x before 7.0.15, and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (buffer over-read and application crash) via crafted serialized data that is mishandled in a finish_nested_data call.
CVE-2016-10162	The php_wddx_pop_element function in ext/wddx/wddx.c in PHP 7.0.x before 7.0.15 and 7.1.x before 7.1.1 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via an inapplicable class name in a wddxPacket XML document, leading to mishandling in a wddx_deserialize call.
CVE-2016-10164	Multiple integer overflows in libXpm before 3.5.12, when a program requests parsing XPM extensions on a 64-bit platform, allow remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via (1) the number of extensions or (2) their concatenated length in a crafted XPM file, which triggers a heap-based buffer overflow.
CVE-2016-10165	The Type_MLU_Read function in cmstypes.c in Little CMS (aka lcms2) allows remote attackers to obtain sensitive information or cause a denial of service via an image with a crafted ICC profile, which triggers an out-of-bounds heap read.
CVE-2016-10166	Integer underflow in the _gdContributionsAlloc function in gd_interpolation.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to have

	unspecified impact via vectors related to decrementing the u variable.
CVE-2016-10167	The gdImageCreateFromGd2Ctx function in gd_gd2.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to cause a denial of service (application crash) via a crafted image file.
CVE-2016-10168	Integer overflow in gd_io.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to have unspecified impact via vectors involving the number of horizontal and vertical chunks in an image.
CVE-2016-10169	The read_code function in read_words.c in Wavpack before 5.1.0 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted WV file.
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-2016-10195	The name_parse function in evdns.c in libevent before 2.1.6-beta allows remote attackers to have unspecified impact via vectors involving the label_len variable, which triggers an out-of-bounds stack read.
CVE-2016-10196	Stack-based buffer overflow in the evutil_parse_sockaddr_port function in evutil.c in libevent before 2.1.6-beta allows attackers to cause a denial of service (segmentation fault) via vectors involving a long string in brackets in the ip_as_string argument.
CVE-2016-10197	The search_make_new function in evdns.c in libevent before 2.1.6-beta allows attackers to cause a denial of service (out-of-bounds read) via an empty hostname.
CVE-2016-10198	The gst_aac_parse_sink_setcaps function in gst/audioparsers/gstaacparse.c in gst-plugins-good in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (invalid memory read and crash) via a crafted audio file.

CVE-2016-10199	The qtdemux_tag_add_str_full function in gst/isomp4/qtdemux.c in gst-plugins-good in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted tag value.
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-2016-10208	The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.9.8 does not properly validate meta block groups, which allows physically proximate attackers to cause a denial of service (out-of-bounds read and system crash) via a crafted ext4 image.
CVE-2016-10209	The archive_wstring_append_from_mbs function in archive_string.c in libarchive 3.2.2 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted archive file.
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-2016-10217	The pdf14_open function in base/gdevp14.c in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (use-after-free and application crash) via a crafted file that is mishandled in the color management module.
CVE-2016-10219	The intersect function in base/gxfill.c in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted file.
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-2016-10220	The gs_makewordimagedevice function in base/gsdevmem.c in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file that is mishandled in the PDF Transparency module.
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-2016-10243	TeX Live allows remote attackers to execute arbitrary commands by leveraging inclusion of mpost in shell_escape_commands in the texmf.cnf config file.
CVE-2016-10244	The parse_charstrings function in type1/t1load.c in FreeType 2 before 2.7 does not ensure that a font contains a glyph name, which allows remote attackers to cause a denial of service (heap-based buffer over-read) or possibly have unspecified other impact via a crafted file.
CVE-2016-10248	The jpc_tsfb_synthesize function in jpc_tsfb.c in JasPer before 1.900.9 allows remote attackers to cause a denial of service (NULL pointer dereference) via vectors involving an empty sequence.
CVE-2016-10249	Integer overflow in the jpc_dec_tiledecode function in jpc_dec.c in JasPer before 1.900.12 allows remote attackers to have unspecified impact via a crafted image file, which triggers a heap-based buffer overflow.
CVE-2016-1025	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to

	execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-10250	The jp2_colr_destroy function in jp2_cod.c in JasPer before 1.900.13 allows remote attackers to cause a denial of service (NULL pointer dereference) by leveraging incorrect cleanup of JP2 box data on error. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8887.
CVE-2016-10251	Integer overflow in the jpc_pi_nextcprl function in jpc_t2cod.c in JasPer before 1.900.20 allows remote attackers to have unspecified impact via a crafted file, which triggers use of an uninitialized value.
CVE-2016-10253	An issue was discovered in Erlang/OTP 18.x. Erlang's generation of compiled regular expressions is vulnerable to a heap overflow. Regular expressions using a malformed extpattern can indirectly specify an offset that is used as an array index. This ordinal permits arbitrary regions within the erts_alloc arena to be both read and written to.
CVE-2016-10254	The allocate_elf function in common.h in elfutils before 0.168 allows remote attackers to cause a denial of service (crash) via a crafted ELF file, which triggers a memory allocation failure.
CVE-2016-10255	The __libelf_set_rawdata_wrlock function in elf_getdata.c in elfutils before 0.168 allows remote attackers to cause a denial of service (crash) via a crafted (1) sh_off or (2) sh_size ELF header value, which triggers a memory allocation failure.
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-2016-10266	LibTIFF 4.0.7 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted TIFF image, related to libtiff/tif_read.c:351:22.
CVE-2016-10267	LibTIFF 4.0.7 allows remote attackers to cause a denial of service (divide-by-zero error and application

	crash) via a crafted TIFF image, related to libtiff/tif_ojpeg.c:816:8.
CVE-2016-10268	tools/tiffcp.c in LibTIFF 4.0.7 allows remote attackers to cause a denial of service (integer underflow and heap-based buffer under-read) or possibly have unspecified other impact via a crafted TIFF image, related to "READ of size 78490" and libtiff/tif_unix.c:115:23.
CVE-2016-10269	LibTIFF 4.0.7 allows remote attackers to cause a denial of service (heap-based buffer over-read) or possibly have unspecified other impact via a crafted TIFF image, related to "READ of size 512" and libtiff/tif_unix.c:340:2.
CVE-2016-1027	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1028, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1028	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1029, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1029	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1032, and CVE-2016-1033.
CVE-2016-1030	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to bypass intended access restrictions via unspecified vectors.
CVE-2016-1031	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different

	vulnerability than CVE-2016-1011, CVE-2016-1013, CVE-2016-1016, and CVE-2016-1017.
CVE-2016-10317	The fill_threshhold_buffer function in base/gxht_thresh.c in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted PostScript document.
CVE-2016-1032	Adobe Flash Player before 18.0.0.343 and 19.x through 21.x before 21.0.0.213 on Windows and OS X and before 11.2.202.616 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1012, CVE-2016-1020, CVE-2016-1021, CVE-2016-1022, CVE-2016-1023, CVE-2016-1024, CVE-2016-1025, CVE-2016-1026, CVE-2016-1027, CVE-2016-1028, CVE-2016-1029, and CVE-2016-1033.
CVE-2016-10327	LibreOffice before 2016-12-22 has an out-of-bounds write caused by a heap-based buffer overflow related to the EnhWMFReader::ReadEnhWMF function in vcl/source/filter/wmf/enhwmf.cxx.
CVE-2016-10328	FreeType 2 before 2016-12-16 has an out-of-bounds write caused by a heap-based buffer overflow related to the cff_parser_run function in cff/cffparse.c.
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-2016-10349	The archive_le32dec function in archive_endian.h in libarchive 3.2.2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file.
CVE-2016-10350	The archive_read_format_cab_read_header function in archive_read_support_format_cab.c in libarchive 3.2.2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted file.
CVE-2016-10371	The TIFFWriteDirectoryTagCheckedRational function in tif_dirwrite.c in LibTIFF 4.0.6 allows remote attackers to cause a denial of service (assertion failure and application exit) via a crafted TIFF file.
CVE-2016-10516	Cross-site scripting (XSS) vulnerability in the render_full function in debug/tbtools.py in the debugger in Pallets

	Werkzeug before 0.11.11 (as used in Pallets Flask and other products) allows remote attackers to inject arbitrary web script or HTML via a field that contains an exception message.
CVE-2016-10708	sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.
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-2016-10714	In zsh before 5.3, an off-by-one error resulted in undersized buffers that were intended to support PATH_MAX characters.
CVE-2016-10727	camel/providers/imapx/camel-imapx-server.c in the IMAPx component in GNOME evolution-data-server before 3.21.2 proceeds with cleartext data containing a password if the client wishes to use STARTTLS but the server will not use STARTTLS, which makes it easier for remote attackers to obtain sensitive information by sniffing the network. The server code was intended to report an error and not proceed, but the code was written incorrectly.
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-2016-1234	Stack-based buffer overflow in the glob implementation in GNU C Library (aka glibc) before 2.24, when GLOB_ALTDIRFUNC is used, allows context-dependent attackers to cause a denial of service (crash) via a long name.
CVE-2016-1237	nfsd in the Linux kernel through 4.6.3 allows local users to bypass intended file-permission restrictions by setting a POSIX ACL, related to nfs2acl.c, nfs3acl.c, and nfs4acl.c.
CVE-2016-1240	The Tomcat init script in the tomcat7 package before 7.0.56-3+deb8u4 and tomcat8 package before 8.0.14-1+deb8u3 on Debian jessie and the tomcat6 and libtomcat6-java packages before 6.0.35-1ubuntu3.8 on Ubuntu 12.04 LTS, the tomcat7 and libtomcat7-java packages before 7.0.52-1ubuntu0.7 on Ubuntu 14.04 LTS, and tomcat8 and libtomcat8-java packages before 8.0.32-1ubuntu1.2 on Ubuntu 16.04 LTS allows local users with access to the tomcat account to gain root privileges via a symlink attack on the Catalina log file, as demonstrated by /var/log/tomcat7/catalina.out.
CVE-2016-1245	It was discovered that the zebra daemon in Quagga before 1.0.20161017 suffered from a stack-based buffer overflow when processing IPv6 Neighbor Discovery messages. The root cause was relying on BUFSIZ to be compatible with a message size; however, BUFSIZ is system-dependent.
CVE-2016-1247	The nginx package before 1.6.2-5+deb8u3 on Debian jessie, the nginx packages before 1.4.6-1ubuntu3.6 on Ubuntu 14.04 LTS, before 1.10.0-0ubuntu0.16.04.3 on Ubuntu 16.04 LTS, and before 1.10.1-0ubuntu1.1 on Ubuntu 16.10, and the nginx ebuild before 1.10.2-r3 on Gentoo allow local users with access to the web server user account to gain root privileges via a symlink attack on the error log.
CVE-2016-1248	vim before patch 8.0.0056 does not properly validate values for the 'filetype', 'syntax' and 'keymap' options,

	which may result in the execution of arbitrary code if a file with a specially crafted modeline is opened.
CVE-2016-1252	The apt package in Debian jessie before 1.0.9.8.4, in Debian unstable before 1.4~beta2, in Ubuntu 14.04 LTS before 1.0.1ubuntu2.17, in Ubuntu 16.04 LTS before 1.2.15ubuntu0.2, and in Ubuntu 16.10 before 1.3.2ubuntu0.1 allows man-in-the-middle attackers to bypass a repository-signing protection mechanism by leveraging improper error handling when validating InRelease file signatures.
CVE-2016-1255	The pg_ctlcluster script in postgresql-common package in Debian wheezy before 134wheezy5, in Debian jessie before 165+deb8u2, in Debian unstable before 178, in Ubuntu 12.04 LTS before 129ubuntu1.2, in Ubuntu 14.04 LTS before 154ubuntu1.1, in Ubuntu 16.04 LTS before 173ubuntu0.1, in Ubuntu 17.04 before 179ubuntu0.1, and in Ubuntu 17.10 before 184ubuntu1.1 allows local users to gain root privileges via a symlink attack on a logfile in /var/log/postgresql.
CVE-2016-1371	ClamAV (aka Clam AntiVirus) before 0.99.2 allows remote attackers to cause a denial of service (application crash) via a crafted mew packer executable.
CVE-2016-1372	ClamAV (aka Clam AntiVirus) before 0.99.2 allows remote attackers to cause a denial of service (application crash) via a crafted 7z file.
CVE-2016-1405	libclamav in ClamAV (aka Clam AntiVirus), as used in Advanced Malware Protection (AMP) on Cisco Email Security Appliance (ESA) devices before 9.7.0-125 and Web Security Appliance (WSA) devices before 9.0.1-135 and 9.1.x before 9.1.1-041, allows remote attackers to cause a denial of service (AMP process restart) via a crafted document, aka Bug IDs CSCuv78533 and CSCuw60503.
CVE-2016-1541	Heap-based buffer overflow in the zip_read_mac_metadata function in archive_read_support_format_zip.c in libarchive before 3.2.0 allows remote attackers to execute arbitrary code via crafted entry-size values in a ZIP archive.
CVE-2016-1547	An off-path attacker can cause a preemptible client association to be demobilized in NTP 4.2.8p4 and earlier and NTPSec a5fb34b9cc89b92a8fef2f459004865c93bb7f92 by sending a crypto NAK packet to a victim client with a spoofed source address of an existing associated peer. This is true even if authentication is enabled.
CVE-2016-1548	An attacker can spoof a packet from a legitimate ntpd server with an origin timestamp that matches the peer->dst timestamp recorded for that server. After making this switch, the

	client in NTP 4.2.8p4 and earlier and NTPSec aa48d001683e5b791a743ec9c575aaf7d867a2b0c will reject all future legitimate server responses. It is possible to force the victim client to move time after the mode has been changed. ntpq gives no indication that the mode has been switched.
CVE-2016-1550	An exploitable vulnerability exists in the message authentication functionality of libntp in ntp 4.2.8p4 and NTPSec a5fb34b9cc89b92a8fef2f459004865c93bb7f92. An attacker can send a series of crafted messages to attempt to recover the message digest key.
CVE-2016-1578	Use-after-free vulnerability in Oxide allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via unspecified vectors, related to responding synchronously to permission requests.
CVE-2016-1580	The setup_snappy_os_mounts function in the ubuntu-core-launcher package before 1.0.27.1 improperly determines the mount point of bind mounts when using snaps, which might allow remote attackers to obtain sensitive information or gain privileges via a snap with a name starting with "ubuntu-core."
CVE-2016-1581	LXD before 2.0.2 uses world-readable permissions for /var/lib/lxd/zfs.img when setting up a loop based ZFS pool, which allows local users to copy and read data from arbitrary containers via unspecified vectors.
CVE-2016-1582	LXD before 2.0.2 does not properly set permissions when switching an unprivileged container into privileged mode, which allows local users to access arbitrary world readable paths in the container directory via unspecified vectors.
CVE-2016-1583	The ecryptfs_privileged_open function in fs/ecryptfs/kthread.c in the Linux kernel before 4.6.3 allows local users to gain privileges or cause a denial of service (stack memory consumption) via vectors involving crafted mmap calls for /proc pathnames, leading to recursive pagefault handling.
CVE-2016-1612	The LoadIC::UpdateCaches function in ic/ic.cc in Google V8, as used in Google Chrome before 48.0.2564.82, does not ensure receiver compatibility before performing a cast of an unspecified variable, which allows remote attackers to cause a denial of service or possibly have unknown other impact via crafted JavaScript code.
CVE-2016-1613	Multiple use-after-free vulnerabilities in the formfiller implementation in PDFium, as used in Google Chrome before 48.0.2564.82, allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted PDF document, related to improper

	tracking of the destruction of (1) IPWL_FocusHandler and (2) IPWL_Provider objects.
CVE-2016-1614	The UnacceleratedImageBufferSurface class in WebKit/Source/platform/graphics/UnacceleratedImageBufferSurface.cpp in Blink, as used in Google Chrome before 48.0.2564.82, mishandles the initialization mode, which allows remote attackers to obtain sensitive information from process memory via a crafted web site.
CVE-2016-1615	The Omnibox implementation in Google Chrome before 48.0.2564.82 allows remote attackers to spoof a document's origin via unspecified vectors.
CVE-2016-1616	The CustomButton::AcceleratorPressed function in ui/views/controls/button/custom_button.cc in Google Chrome before 48.0.2564.82 allows remote attackers to spoof URLs via vectors involving an unfocused custom button.
CVE-2016-1617	The CSPSource::schemeMatches function in WebKit/Source/core/frame/csp/CSPSource.cpp in the Content Security Policy (CSP) implementation in Blink, as used in Google Chrome before 48.0.2564.82, does not apply http policies to https URLs and does not apply ws policies to wss URLs, which makes it easier for remote attackers to determine whether a specific HSTS web site has been visited by reading a CSP report.
CVE-2016-1618	Blink, as used in Google Chrome before 48.0.2564.82, does not ensure that a proper cryptographicallyRandomValues random number generator is used, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via unspecified vectors.
CVE-2016-1619	Multiple integer overflows in the (1) sycc422_to_rgb and (2) sycc444_to_rgb functions in fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 48.0.2564.82, allow remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted PDF document.
CVE-2016-1620	Multiple unspecified vulnerabilities in Google Chrome before 48.0.2564.82 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-1622	The Extensions subsystem in Google Chrome before 48.0.2564.109 does not prevent use of the Object.defineProperty method to override intended extension behavior, which allows remote attackers to bypass the Same Origin Policy via crafted JavaScript code.
CVE-2016-1623	The DOM implementation in Google Chrome before 48.0.2564.109 does not properly restrict frame-attach

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

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

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

CVE-2016-1647	Use-after-free vulnerability in the RenderWidgetHostImpl::Destroy function in content/browser/renderer_host/render_widget_host_impl.cc in the Navigation implementation in Google Chrome before 49.0.2623.108 allows remote attackers to cause a denial of service or possibly have unspecified other impact via unknown vectors.
CVE-2016-1648	Use-after-free vulnerability in the GetLoadTimes function in renderer/loadtimes_extension_bindings.cc in the Extensions implementation in Google Chrome before 49.0.2623.108 allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code.
CVE-2016-1649	The Program::getUniformInternal function in Program.cpp in libANGLE, as used in Google Chrome before 49.0.2623.108, does not properly handle a certain data-type mismatch, which allows remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via crafted shader stages.
CVE-2016-1650	The PageCaptureSaveAsMHTMLFunction::ReturnFailure function in browser/extensions/api/page_capture/page_capture_api.cc in Google Chrome before 49.0.2623.108 allows attackers to cause a denial of service or possibly have unspecified other impact by triggering an error in creating an MHTML document.
CVE-2016-1651	fxcodec/codec/fx_codec_jpx_opj.cpp in PDFium, as used in Google Chrome before 50.0.2661.75, does not properly implement the sycc420_to_rgb and sycc422_to_rgb functions, which allows remote attackers to obtain sensitive information from process memory or cause a denial of service (out-of-bounds read) via crafted JPEG 2000 data in a PDF document.
CVE-2016-1652	Cross-site scripting (XSS) vulnerability in the ModuleSystem::RequireForJsInner function in extensions/renderer/module_system.cc in the Extensions subsystem in Google Chrome before 50.0.2661.75 allows remote attackers to inject arbitrary web script or HTML via a crafted web site, aka "Universal XSS (UXSS)."
CVE-2016-1653	The LoadBuffer implementation in Google V8, as used in Google Chrome before 50.0.2661.75, mishandles data types, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JavaScript code that triggers an out-of-bounds write operation, related to compiler/pipeline.cc and compiler/simplified-lowering.cc.
CVE-2016-1654	The media subsystem in Google Chrome before 50.0.2661.75 does not initialize an unspecified data

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

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

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

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

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

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

	consider object lifetimes during progress observation, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted web site.
CVE-2016-1709	Heap-based buffer overflow in the ByteArray::Get method in data/byte_array.cc in Google sfntly before 2016-06-10, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted SFNT font.
CVE-2016-1710	The ChromeClientImpl::createWindow method in WebKit/Source/web/ChromeClientImpl.cpp in Blink, as used in Google Chrome before 52.0.2743.82, does not prevent window creation by a deferred frame, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1711	WebKit/Source/core/loader/FrameLoader.cpp in Blink, as used in Google Chrome before 52.0.2743.82, does not disable frame navigation during a detach operation on a DocumentLoader object, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-1762	The xmlNextChar function in libxml2 before 2.9.4 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1833	The htmlCurrentChar function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1834	Heap-based buffer overflow in the xmlStrncat function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2016-1835	Use-after-free vulnerability in the xmlSAX2AttributeNs function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2 and OS X before 10.11.5, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1836	Use-after-free vulnerability in the xmlDictComputeFastKey function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1837	Multiple use-after-free vulnerabilities in the (1) htmlPArsePubidLiteral and (2) htmlParseSystemiteral

	functions in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allow remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1838	The xmlPArserPrintFileContextInternal function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1839	The xmlDictAddString function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1840	Heap-based buffer overflow in the xmlFAParsePosCharGroup function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2016-1841	libxslt, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.
CVE-2016-1854	WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1855, CVE-2016-1856, and CVE-2016-1857.
CVE-2016-1856	WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1854, CVE-2016-1855, and CVE-2016-1857.
CVE-2016-1857	WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-1854, CVE-2016-1855, and CVE-2016-1856.
CVE-2016-1858	WebKit, as used in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1, improperly tracks taint attributes, which allows remote attackers to obtain sensitive information via a crafted web site.

CVE-2016-1859	The WebKit Canvas implementation in Apple iOS before 9.3.2, Safari before 9.1.1, and tvOS before 9.2.1 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.
CVE-2016-1867	The jpc_pi_nextcprl function in JasPer 1.900.1 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG 2000 image.
CVE-2016-1938	The s_mp_div function in lib/freebl/mpi/mpi.c in Mozilla Network Security Services (NSS) before 3.21, as used in Mozilla Firefox before 44.0, improperly divides numbers, which might make it easier for remote attackers to defeat cryptographic protection mechanisms by leveraging use of the (1) mp_div or (2) mp_exptmod function.
CVE-2016-1950	Heap-based buffer overflow in Mozilla Network Security Services (NSS) before 3.19.2.3 and 3.20.x and 3.21.x before 3.21.1, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to execute arbitrary code via crafted ASN.1 data in an X.509 certificate.
CVE-2016-1951	Multiple integer overflows in io/prprf.c in Mozilla Netscape Portable Runtime (NSPR) before 4.12 allow remote attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a long string to a PR_*printf function.
CVE-2016-1952	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2016-1954	The nsCSPContext::SendReports function in dom/security/nsCSPContext.cpp in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 does not prevent use of a non-HTTP report-uri for a Content Security Policy (CSP) violation report, which allows remote attackers to cause a denial of service (data overwrite) or possibly gain privileges by specifying a URL of a local file.
CVE-2016-1957	Memory leak in libstagefright in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to cause a denial of service (memory consumption) via an MPEG-4 file that triggers a delete operation on an array.
CVE-2016-1960	Integer underflow in the nsHtml5TreeBuilder class in the HTML5 string parser in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to execute arbitrary code or cause a denial

	of service (use-after-free) by leveraging mishandling of end tags, as demonstrated by incorrect SVG processing, aka ZDI-CAN-3545.
CVE-2016-1961	Use-after-free vulnerability in the nsHTMLDocument::SetBody function in dom/html/nsHTMLDocument.cpp in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to execute arbitrary code by leveraging mishandling of a root element, aka ZDI-CAN-3574.
CVE-2016-1964	Use-after-free vulnerability in the AtomicBaseIncDec function in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by leveraging mishandling of XML transformations.
CVE-2016-1966	The nsNPObjWrapper::GetNewOrUsed function in dom/plugins/base/nsJSNPRuntime.cpp in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 allows remote attackers to execute arbitrary code or cause a denial of service (invalid pointer dereference and memory corruption) via a crafted NPAPI plugin.
CVE-2016-1974	The nsScannerString::AppendUnicodeTo function in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7 does not verify that memory allocation succeeds, which allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds read) via crafted Unicode data in an HTML, XML, or SVG document.
CVE-2016-1977	The Machine::Code::decoder::analysis::set_ref function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to execute arbitrary code or cause a denial of service (stack memory corruption) via a crafted Graphite smart font.
CVE-2016-1978	Use-after-free vulnerability in the ssl3_HandleECDHServerKeyExchange function in Mozilla Network Security Services (NSS) before 3.21, as used in Mozilla Firefox before 44.0, allows remote attackers to cause a denial of service or possibly have unspecified other impact by making an SSL (1) DHE or (2) ECDHE handshake at a time of high memory consumption.
CVE-2016-1979	Use-after-free vulnerability in the PK11_ImportDERPrivateKeyInfoAndReturnKey function in Mozilla Network Security Services (NSS) before 3.21.1, as used in Mozilla Firefox before 45.0, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted key data with DER encoding.

CVE-2016-2047	The ssl_verify_server_cert function in sql-common/client.c in MariaDB before 5.5.47, 10.0.x before 10.0.23, and 10.1.x before 10.1.10; Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier; and Percona Server do not properly verify that the server hostname matches a domain name in the subject's Common Name (CN) or subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via a "/CN=" string in a field in a certificate, as demonstrated by "/OU=/CN=bar.com/CN=foo.com."
CVE-2016-2051	Multiple unspecified vulnerabilities in Google V8 before 4.8.271.17, as used in Google Chrome before 48.0.2564.82, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-2052	Multiple unspecified vulnerabilities in HarfBuzz before 1.0.6, as used in Google Chrome before 48.0.2564.82, allow attackers to cause a denial of service or possibly have other impact via crafted data, as demonstrated by a buffer over-read resulting from an inverted length check in hb-ot-font.cc, a different issue than CVE-2015-8947.
CVE-2016-2073	The htmlParseNameComplex function in HTMLparser.c in libxml2 allows attackers to cause a denial of service (out-of-bounds read) via a crafted XML document.
CVE-2016-2089	The jas_matrix_clip function in jas_seq.c in JasPer 1.900.1 allows remote attackers to cause a denial of service (invalid read and application crash) via a crafted JPEG 2000 image.
CVE-2016-2105	Integer overflow in the EVP_EncodeUpdate function in crypto/evp/encode.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.
CVE-2016-2106	Integer overflow in the EVP_EncryptUpdate function in crypto/evp/evp_enc.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of data.
CVE-2016-2107	The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session. NOTE: this vulnerability exists because of an incorrect fix for CVE-2013-0169.
CVE-2016-2108	The ASN.1 implementation in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service

	(buffer underflow and memory corruption) via an ANY field in crafted serialized data, aka the "negative zero" issue.
CVE-2016-2109	The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in the ASN.1 BIO implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.
CVE-2016-2110	The NTLMSSP authentication implementation in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 allows man-in-the-middle attackers to perform protocol-downgrade attacks by modifying the client-server data stream to remove application-layer flags or encryption settings, as demonstrated by clearing the NTLMSSP_NEGOTIATE_SEAL or NTLMSSP_NEGOTIATE_SIGN option to disrupt LDAP security.
CVE-2016-2111	The NETLOGON service in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2, when a domain controller is configured, allows remote attackers to spoof the computer name of a secure channel's endpoint, and obtain sensitive session information, by running a crafted application and leveraging the ability to sniff network traffic, a related issue to CVE-2015-0005.
CVE-2016-2112	The bundled LDAP client library in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not recognize the "client ldap sasl wrapping" setting, which allows man-in-the-middle attackers to perform LDAP protocol-downgrade attacks by modifying the client-server data stream.
CVE-2016-2113	Samba 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not verify X.509 certificates from TLS servers, which allows man-in-the-middle attackers to spoof LDAPS and HTTPS servers and obtain sensitive information via a crafted certificate.
CVE-2016-2114	The SMB1 protocol implementation in Samba 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not recognize the "server signing = mandatory" setting, which allows man-in-the-middle attackers to spoof SMB servers by modifying the client-server data stream.
CVE-2016-2115	Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 does not require SMB signing within a DCERPC session over ncacn_np, which allows man-in-the-middle attackers to spoof SMB clients by modifying the client-server data stream.
CVE-2016-2117	The atl2_probe function in drivers/net/ethernet/atheros/atlx/atl2.c in the Linux kernel through 4.5.2 incorrectly enables scatter/gather I/O, which allows remote

	attackers to obtain sensitive information from kernel memory by reading packet data.
CVE-2016-2118	The MS-SAMR and MS-LSAD protocol implementations in Samba 3.x and 4.x before 4.2.11, 4.3.x before 4.3.8, and 4.4.x before 4.4.2 mishandle DCERPC connections, which allows man-in-the-middle attackers to perform protocol-downgrade attacks and impersonate users by modifying the client-server data stream, aka "BADLOCK."
CVE-2016-2119	libcli/smb/smbXcli_base.c in Samba 4.x before 4.2.14, 4.3.x before 4.3.11, and 4.4.x before 4.4.5 allows man-in-the-middle attackers to bypass a client-signing protection mechanism, and consequently spoof SMB2 and SMB3 servers, via the (1) SMB2_SESSION_FLAG_IS_GUEST or (2) SMB2_SESSION_FLAG_IS_NULL flag.
CVE-2016-2123	A flaw was found in samba versions 4.0.0 to 4.5.2. The Samba routine ndr_pull_dnsp_name contains an integer wrap problem, leading to an attacker-controlled memory overwrite. ndr_pull_dnsp_name parses data from the Samba Active Directory ldb database. Any user who can write to the dnsRecord attribute over LDAP can trigger this memory corruption. By default, all authenticated LDAP users can write to the dnsRecord attribute on new DNS objects. This makes the defect a remote privilege escalation.
CVE-2016-2125	It was found that Samba before versions 4.5.3, 4.4.8, 4.3.13 always requested forwardable tickets when using Kerberos authentication. A service to which Samba authenticated using Kerberos could subsequently use the ticket to impersonate Samba to other services or domain users.
CVE-2016-2126	Samba version 4.0.0 up to 4.5.2 is vulnerable to privilege elevation due to incorrect handling of the PAC (Privilege Attribute Certificate) checksum. A remote, authenticated, attacker can cause the winbindd process to crash using a legitimate Kerberos ticket. A local service with access to the winbindd privileged pipe can cause winbindd to cache elevated access permissions.
CVE-2016-2150	SPICE allows local guest OS users to read from or write to arbitrary host memory locations via crafted primary surface parameters, a similar issue to CVE-2015-5261.
CVE-2016-2161	In Apache HTTP Server versions 2.4.0 to 2.4.23, malicious input to mod_auth_digest can cause the server to crash, and each instance continues to crash even for subsequently valid requests.
CVE-2016-2167	The canonicalize_username function in svnserve/cyrus_auth.c in Apache Subversion before 1.8.16 and 1.9.x before 1.9.4, when Cyrus SASL authentication is used, allows remote attackers to authenticate and

	bypass intended access restrictions via a realm string that is a prefix of an expected repository realm string.
CVE-2016-2177	OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.
CVE-2016-2178	The dsa_sign_setup function in crypto/dsa/dsa_ossl.c in OpenSSL through 1.0.2h does not properly ensure the use of constant-time operations, which makes it easier for local users to discover a DSA private key via a timing side-channel attack.
CVE-2016-2179	The DTLS implementation in OpenSSL before 1.1.0 does not properly restrict the lifetime of queue entries associated with unused out-of-order messages, which allows remote attackers to cause a denial of service (memory consumption) by maintaining many crafted DTLS sessions simultaneously, related to d1_lib.c, statem_dtls.c, statem_lib.c, and statem_srvr.c.
CVE-2016-2180	The TS_OBJ_print_bio function in crypto/ts/ts_lib.c in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation in OpenSSL through 1.0.2h allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted time-stamp file that is mishandled by the "openssl ts" command.
CVE-2016-2181	The Anti-Replay feature in the DTLS implementation in OpenSSL before 1.1.0 mishandles early use of a new epoch number in conjunction with a large sequence number, which allows remote attackers to cause a denial of service (false-positive packet drops) via spoofed DTLS records, related to rec_layer_d1.c and ssl3_record.c.
CVE-2016-2182	The BN_bn2dec function in crypto/bn/bn_print.c in OpenSSL before 1.1.0 does not properly validate division results, which allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2016-2183	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.

CVE-2016-2184	The create_fixed_stream_quirk function in sound/usb/quirks.c in the snd-usb-audio driver in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference or double free, and system crash) via a crafted endpoints value in a USB device descriptor.
CVE-2016-2185	The ati_remote2_probe function in drivers/input/misc/ati_remote2.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.
CVE-2016-2186	The powermate_probe function in drivers/input/misc/powermate.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.
CVE-2016-2187	The gtco_probe function in drivers/input/tablet/gtco.c in the Linux kernel through 4.5.2 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.
CVE-2016-2188	The iowarrior_probe function in drivers/usb/misc/iowarrior.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.
CVE-2016-2391	The ohci_bus_start function in the USB OHCI emulation support (hw/usb/hcd-ohci.c) in QEMU allows local guest OS administrators to cause a denial of service (NULL pointer dereference and QEMU process crash) via vectors related to multiple eof_timers.
CVE-2016-2392	The is_rndis function in the USB Net device emulator (hw/usb/dev-network.c) in QEMU before 2.5.1 does not properly validate USB configuration descriptor objects, which allows local guest OS administrators to cause a denial of service (NULL pointer dereference and QEMU process crash) via vectors involving a remote NDIS control message packet.
CVE-2016-2516	NTP before 4.2.8p7 and 4.3.x before 4.3.92, when mode7 is enabled, allows remote attackers to cause a denial of service (ntpd abort) by using the same IP address multiple times in an unconfig directive.
CVE-2016-2518	The MATCH_ASSOC function in NTP before version 4.2.8p9 and 4.3.x before 4.3.92 allows remote attackers to cause an out-of-bounds reference via an addpeer request with a large hmode value.

CVE-2016-2519	ntpd in NTP before 4.2.8p7 and 4.3.x before 4.3.92 allows remote attackers to cause a denial of service (ntpd abort) by a large request data value, which triggers the ctl_getitem function to return a NULL value.
CVE-2016-2538	Multiple integer overflows in the USB Net device emulator (hw/usb/dev-network.c) in QEMU before 2.5.1 allow local guest OS administrators to cause a denial of service (QEMU process crash) or obtain sensitive host memory information via a remote NDIS control message packet that is mishandled in the (1) rndis_query_response, (2) rndis_set_response, or (3) usb_net_handle_dataout function.
CVE-2016-2569	Squid 3.x before 3.5.15 and 4.x before 4.0.7 does not properly append data to String objects, which allows remote servers to cause a denial of service (assertion failure and daemon exit) via a long string, as demonstrated by a crafted HTTP Vary header.
CVE-2016-2570	The Edge Side Includes (ESI) parser in Squid 3.x before 3.5.15 and 4.x before 4.0.7 does not check buffer limits during XML parsing, which allows remote HTTP servers to cause a denial of service (assertion failure and daemon exit) via a crafted XML document, related to esi/CustomParser.cc and esi/CustomParser.h.
CVE-2016-2571	http.cc in Squid 3.x before 3.5.15 and 4.x before 4.0.7 proceeds with the storage of certain data after a response-parsing failure, which allows remote HTTP servers to cause a denial of service (assertion failure and daemon exit) via a malformed response.
CVE-2016-2774	ISC DHCP 4.1.x before 4.1-ESV-R13 and 4.2.x and 4.3.x before 4.3.4 does not restrict the number of concurrent TCP sessions, which allows remote attackers to cause a denial of service (INSIST assertion failure or request-processing outage) by establishing many sessions.
CVE-2016-2776	buffer.c in named in ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 does not properly construct responses, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.
CVE-2016-2790	The graphite2::TtfUtil::GetTableInfo function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, does not initialize memory for an unspecified data structure, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted Graphite smart font.
CVE-2016-2791	The graphite2::GlyphCache::glyph function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote

	attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font.
CVE-2016-2792	The graphite2::Slot::getAttr function in Slot.cpp in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font, a different vulnerability than CVE-2016-2800.
CVE-2016-2793	CachedCmap.cpp in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font.
CVE-2016-2794	The graphite2::TtfUtil::CmapSubtable12NextCodepoint function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font.
CVE-2016-2795	The graphite2::FileFace::get_table_fn function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, does not initialize memory for an unspecified data structure, which allows remote attackers to cause a denial of service or possibly have unknown other impact via a crafted Graphite smart font.
CVE-2016-2796	Heap-based buffer overflow in the graphite2::vm::Machine::Code::Code function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Graphite smart font.
CVE-2016-2797	The graphite2::TtfUtil::CmapSubtable12Lookup function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font, a different vulnerability than CVE-2016-2801.
CVE-2016-2798	The graphite2::GlyphCache::Loader::Loader function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font.
CVE-2016-2799	Heap-based buffer overflow in the graphite2::Slot::setAttr function in Graphite 2 before

	1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted Graphite smart font.
CVE-2016-2800	The graphite2::Slot::getAttr function in Slot.cpp in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font, a different vulnerability than CVE-2016-2792.
CVE-2016-2801	The graphite2::TtfUtil::CmapSubtable12Lookup function in TtfUtil.cpp in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font, a different vulnerability than CVE-2016-2797.
CVE-2016-2802	The graphite2::TtfUtil::CmapSubtable4NextCodepoint function in Graphite 2 before 1.3.6, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted Graphite smart font.
CVE-2016-2804	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 46.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2016-2805	Unspecified vulnerability in the browser engine in Mozilla Firefox ESR 38.x before 38.8 allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2016-2806	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 46.0 and Firefox ESR 45.x before 45.1 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2016-2807	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 46.0, Firefox ESR 38.x before 38.8, and Firefox ESR 45.x before 45.1 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2016-2808	The watch implementation in the JavaScript engine in Mozilla Firefox before 46.0, Firefox ESR 38.x before 38.8, and Firefox ESR 45.x before 45.1 allows remote attackers to execute arbitrary code or cause a denial

	of service (generation-count overflow, out-of-bounds HashMap write access, and application crash) via a crafted web site.
CVE-2016-2811	Use-after-free vulnerability in the ServiceWorkerInfo class in the Service Worker subsystem in Mozilla Firefox before 46.0 allows remote attackers to execute arbitrary code via vectors related to the BeginReading method.
CVE-2016-2812	Race condition in the get implementation in the ServiceWorkerManager class in the Service Worker subsystem in Mozilla Firefox before 46.0 allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a crafted web site.
CVE-2016-2814	Heap-based buffer overflow in the stagefright::SampleTable::parseSampleCencInfo function in libstagefright in Mozilla Firefox before 46.0, Firefox ESR 38.x before 38.8, and Firefox ESR 45.x before 45.1 allows remote attackers to execute arbitrary code via crafted CENC offsets that lead to mismanagement of the sizes table.
CVE-2016-2815	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 47.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2016-2816	Mozilla Firefox before 46.0 allows remote attackers to bypass the Content Security Policy (CSP) protection mechanism via the multipart/x-mixed-replace content type.
CVE-2016-2817	The WebExtension sandbox feature in browser/components/extensions/ext-tabs.js in Mozilla Firefox before 46.0 does not properly restrict principal inheritance during chrome.tabs.create and chrome.tabs.update API calls, which allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted extension that accesses a (1) javascript: or (2) data: URL.
CVE-2016-2818	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2016-2819	Heap-based buffer overflow in Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2 allows remote attackers to execute arbitrary code via foreign-context HTML5 fragments, as demonstrated by fragments within an SVG element.

CVE-2016-2820	The Firefox Health Reports (aka FHR or about:healthreport) feature in Mozilla Firefox before 46.0 does not properly restrict the origin of events, which makes it easier for remote attackers to modify sharing preferences by leveraging access to the remote-report IFRAME element.
CVE-2016-2821	Use-after-free vulnerability in the mozilla::dom::Element class in Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2, when contenteditable mode is enabled, allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by triggering deletion of DOM elements that were created in the editor.
CVE-2016-2822	Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2 allow remote attackers to spoof the address bar via a SELECT element with a persistent menu.
CVE-2016-2825	Mozilla Firefox before 47.0 allows remote attackers to bypass the Same Origin Policy and modify the location.host property via an invalid data: URL.
CVE-2016-2827	The mozilla::net::IsValidReferrerPolicy function in Mozilla Firefox before 49.0 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a Content Security Policy (CSP) referrer directive with zero values.
CVE-2016-2828	Use-after-free vulnerability in Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2 allows remote attackers to execute arbitrary code via WebGL content that triggers texture access after destruction of the texture's recycle pool.
CVE-2016-2829	Mozilla Firefox before 47.0 allows remote attackers to spoof permission notifications via a crafted web site that rapidly triggers permission requests, as demonstrated by the microphone permission or the geolocation permission.
CVE-2016-2830	Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 preserve the network connection used for favicon resource retrieval after the associated browser window is closed, which makes it easier for remote web servers to track users by observing network traffic from multiple IP addresses.
CVE-2016-2831	Mozilla Firefox before 47.0 and Firefox ESR 45.x before 45.2 do not ensure that the user approves the fullscreen and pointerlock settings, which allows remote attackers to cause a denial of service (UI outage), or conduct clickjacking or spoofing attacks, via a crafted web site.
CVE-2016-2832	Mozilla Firefox before 47.0 allows remote attackers to discover the list of disabled plugins via a fingerprinting attack involving Cascading Style Sheets (CSS) pseudo-classes.

CVE-2016-2833	Mozilla Firefox before 47.0 ignores Content Security Policy (CSP) directives for cross-domain Java applets, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via a crafted applet.
CVE-2016-2834	Mozilla Network Security Services (NSS) before 3.23, as used in Mozilla Firefox before 47.0, allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2016-2835	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 48.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2016-2836	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via vectors related to Http2Session::Shutdown and SpdySession31::Shutdown, and other vectors.
CVE-2016-2837	Heap-based buffer overflow in the ClearKey Content Decryption Module (CDM) in the Encrypted Media Extensions (EME) API in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 might allow remote attackers to execute arbitrary code by providing a malformed video and leveraging a Gecko Media Plugin (GMP) sandbox bypass.
CVE-2016-2838	Heap-based buffer overflow in the nsBidi::BracketData::AddOpening function in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allows remote attackers to execute arbitrary code via directional content in an SVG document.
CVE-2016-2839	Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 on Linux make cairo _cairo_surface_get_extents calls that do not properly interact with libav header allocation in FFmpeg 0.10, which allows remote attackers to cause a denial of service (application crash) via a crafted video.
CVE-2016-2841	The ne2000_receive function in the NE2000 NIC emulation support (hw/net/ne2000.c) in QEMU before 2.5.1 allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via crafted values for the PSTART and PSTOP registers, involving ring buffer control.
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-2016-2857	The net_checksum_calculate function in net/checksum.c in QEMU allows local guest OS users to cause a denial of service (out-of-bounds heap read and crash) via the payload length in a crafted packet.
CVE-2016-2858	QEMU, when built with the Pseudo Random Number Generator (PRNG) back-end support, allows local guest OS users to cause a denial of service (process crash) via an entropy request, which triggers arbitrary stack based allocation and memory corruption.
CVE-2016-3074	Integer signedness error in GD Graphics Library 2.1.1 (aka libgd or libgd2) allows remote attackers to cause a denial of service (crash) or potentially execute arbitrary code via crafted compressed gd2 data, which triggers a heap-based buffer overflow.
CVE-2016-3078	Multiple integer overflows in php_zip.c in the zip extension in PHP before 7.0.6 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted call to (1) getFromIndex or (2) getFromName in the ZipArchive class.
CVE-2016-3092	The MultipartStream class in Apache Commons Fileupload before 1.3.2, as used in Apache Tomcat 7.x before 7.0.70, 8.x before 8.0.36, 8.5.x before 8.5.3, and 9.x before 9.0.0.M7 and other products, allows remote attackers to cause a denial of service (CPU consumption) via a long boundary string.
CVE-2016-3132	Double free vulnerability in the SplDoublyLinkedList::offsetSet function in ext/spl/spl_dllist.c in PHP 7.x before 7.0.6 allows remote attackers to execute arbitrary code via a crafted index.
CVE-2016-3135	Integer overflow in the xt_alloc_table_info function in net/netfilter/x_tables.c in the Linux kernel through 4.5.2 on 32-bit platforms allows local users to gain privileges or cause a denial of service (heap memory corruption) via an IPT_SO_SET_REPLACE setsockopt call.

CVE-2016-3136	The mct_u232_msr_to_state function in drivers/usb/serial/mct_u232.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted USB device without two interrupt-in endpoint descriptors.
CVE-2016-3137	drivers/usb/serial/cypress_m8.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a USB device without both an interrupt-in and an interrupt-out endpoint descriptor, related to the cypress_generic_port_probe and cypress_open functions.
CVE-2016-3138	The acm_probe function in drivers/usb/class/cdc-acm.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a USB device without both a control and a data endpoint descriptor.
CVE-2016-3140	The digi_port_init function in drivers/usb/serial/digi_acceleport.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (NULL pointer dereference and system crash) via a crafted endpoints value in a USB device descriptor.
CVE-2016-3156	The IPv4 implementation in the Linux kernel before 4.5.2 mishandles destruction of device objects, which allows guest OS users to cause a denial of service (host OS networking outage) by arranging for a large number of IP addresses.
CVE-2016-3157	The __switch_to function in arch/x86/kernel/process_64.c in the Linux kernel does not properly context-switch IOPL on 64-bit PV Xen guests, which allows local guest OS users to gain privileges, cause a denial of service (guest OS crash), or obtain sensitive information by leveraging I/O port access.
CVE-2016-3186	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-2016-3424	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Optimizer.
CVE-2016-3425	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77; Java SE Embedded 8u77; and JRockit R28.3.9 allows remote attackers to affect availability via vectors related to JAXP.

CVE-2016-3426	Unspecified vulnerability in Oracle Java SE 8u77 and Java SE Embedded 8u77 allows remote attackers to affect confidentiality via vectors related to JCE.
CVE-2016-3427	Unspecified vulnerability in Oracle Java SE 6u113, 7u99, and 8u77; Java SE Embedded 8u77; and JRockit R28.3.9 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to JMX.
CVE-2016-3458	Unspecified vulnerability in Oracle Java SE 6u115, 7u101, and 8u92; and Java SE Embedded 8u91 allows remote attackers to affect integrity via vectors related to CORBA.
CVE-2016-3459	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier and MariaDB 10.0.x before 10.0.25 and 10.1.x before 10.1.14 allows remote administrators to affect availability via vectors related to Server: InnoDB.
CVE-2016-3477	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows local users to affect confidentiality, integrity, and availability via vectors related to Server: Parser.
CVE-2016-3486	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote authenticated users to affect availability via vectors related to Server: FTS.
CVE-2016-3500	Unspecified vulnerability in Oracle Java SE 6u115, 7u101, and 8u92; Java SE Embedded 8u91; and JRockit R28.3.10 allows remote attackers to affect availability via vectors related to JAXP, a different vulnerability than CVE-2016-3508.
CVE-2016-3501	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote authenticated users to affect availability via vectors related to Server: Optimizer.
CVE-2016-3508	Unspecified vulnerability in Oracle Java SE 6u115, 7u101, and 8u92; Java SE Embedded 8u91; and JRockit R28.3.10 allows remote attackers to affect availability via vectors related to JAXP, a different vulnerability than CVE-2016-3500.
CVE-2016-3518	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote authenticated users to affect availability via vectors related to Server: Optimizer.
CVE-2016-3521	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows remote authenticated users to affect availability via vectors related to Server: Types.

CVE-2016-3550	Unspecified vulnerability in Oracle Java SE 6u115, 7u101, and 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality via vectors related to Hotspot.
CVE-2016-3587	Unspecified vulnerability in Oracle Java SE 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot.
CVE-2016-3588	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote authenticated users to affect integrity and availability via vectors related to Server: InnoDB.
CVE-2016-3598	Unspecified vulnerability in Oracle Java SE 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Libraries, a different vulnerability than CVE-2016-3610.
CVE-2016-3606	Unspecified vulnerability in Oracle Java SE 7u101 and 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot.
CVE-2016-3610	Unspecified vulnerability in Oracle Java SE 8u92 and Java SE Embedded 8u91 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Libraries, a different vulnerability than CVE-2016-3598.
CVE-2016-3614	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote authenticated users to affect availability via vectors related to Server: Security: Encryption.
CVE-2016-3615	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows remote authenticated users to affect availability via vectors related to Server: DML.
CVE-2016-3616	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-2016-3622	The fpAcc function in tif_predict.c in the tiff2rgba tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (divide-by-zero error) via a crafted TIFF image.
CVE-2016-3623	The rgb2ycbcr tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (divide-by-zero) by setting the (1) v or (2) h parameter to 0.
CVE-2016-3624	The cvtClump function in the rgb2ycbcr tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a

	denial of service (out-of-bounds write) by setting the "-v" option to -1.
CVE-2016-3627	The xmlStringGetNodeList function in tree.c in libxml2 2.9.3 and earlier, when used in recovery mode, allows context-dependent attackers to cause a denial of service (infinite recursion, stack consumption, and application crash) via a crafted XML document.
CVE-2016-3632	The _TIFFVGetField function in tif_dirinfo.c in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted TIFF image.
CVE-2016-3658	The TIFFWriteDirectoryTagLongLong8Array function in tif_dirwrite.c in the tiffset tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via vectors involving the ma variable.
CVE-2016-3672	The arch_pick_mmap_layout function in arch/x86/mm/mmap.c in the Linux kernel through 4.5.2 does not properly randomize the legacy base address, which makes it easier for local users to defeat the intended restrictions on the ADDR_NO_RANDOMIZE flag, and bypass the ASLR protection mechanism for a setuid or setgid program, by disabling stack-consumption resource limits.
CVE-2016-3679	Multiple unspecified vulnerabilities in Google V8 before 4.9.385.33, as used in Google Chrome before 49.0.2623.108, allow attackers to cause a denial of service or possibly have other impact via unknown vectors.
CVE-2016-3689	The ims_pcu_parse_cdc_data function in drivers/input/misc/ims-pcu.c in the Linux kernel before 4.5.1 allows physically proximate attackers to cause a denial of service (system crash) via a USB device without both a master and a slave interface.
CVE-2016-3698	libndp before 1.6, as used in NetworkManager, does not properly validate the origin of Neighbor Discovery Protocol (NDP) messages, which allows remote attackers to conduct man-in-the-middle attacks or cause a denial of service (network connectivity disruption) by advertising a node as a router from a non-local network.
CVE-2016-3705	The (1) xmlParserEntityCheck and (2) xmlParseAttValueComplex functions in parser.c in libxml2 2.9.3 do not properly keep track of the recursion depth, which allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a crafted XML document containing a large number of nested entity references.
CVE-2016-3706	Stack-based buffer overflow in the getaddrinfo function in sysdeps/posix/getaddrinfo.c in the GNU C Library

	(aka glibc or libc6) allows remote attackers to cause a denial of service (crash) via vectors involving hostent conversion. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-4458.
CVE-2016-3710	The VGA module in QEMU improperly performs bounds checking on banked access to video memory, which allows local guest OS administrators to execute arbitrary code on the host by changing access modes after setting the bank register, aka the "Dark Portal" issue.
CVE-2016-3712	Integer overflow in the VGA module in QEMU allows local guest OS users to cause a denial of service (out-of-bounds read and QEMU process crash) by editing VGA registers in VBE mode.
CVE-2016-3713	The msr_mtrr_valid function in arch/x86/kvm/mtrr.c in the Linux kernel before 4.6.1 supports MSR 0x2f8, which allows guest OS users to read or write to the kvm_arch_vcpu data structure, and consequently obtain sensitive information or cause a denial of service (system crash), via a crafted ioctl call.
CVE-2016-3714	The (1) EPHEMERAL, (2) HTTPS, (3) MVG, (4) MSL, (5) TEXT, (6) SHOW, (7) WIN, and (8) PLT coders in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allow remote attackers to execute arbitrary code via shell metacharacters in a crafted image, aka "ImageTragick."
CVE-2016-3715	The EPHEMERAL coder in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allows remote attackers to delete arbitrary files via a crafted image.
CVE-2016-3716	The MSL coder in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allows remote attackers to move arbitrary files via a crafted image.
CVE-2016-3717	The LABEL coder in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allows remote attackers to read arbitrary files via a crafted image.
CVE-2016-3718	The (1) HTTP and (2) FTP coders in ImageMagick before 6.9.3-10 and 7.x before 7.0.1-1 allow remote attackers to conduct server-side request forgery (SSRF) attacks via a crafted image.
CVE-2016-3945	Multiple integer overflows in the (1) cvt_by_strip and (2) cvt_by_tile functions in the tiff2rgba tool in LibTIFF 4.0.6 and earlier, when -b mode is enabled, allow remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted TIFF image, which triggers an out-of-bounds write.
CVE-2016-3947	Heap-based buffer overflow in the Icmp6::Recv function in icmp/Icmp6.cc in the pinger utility in Squid before 3.5.16 and 4.x before 4.0.8 allows remote servers to cause a denial of service (performance degradation or

	transition failures) or write sensitive information to log files via an ICMPv6 packet.
CVE-2016-3948	Squid 3.x before 3.5.16 and 4.x before 4.0.8 improperly perform bounds checking, which allows remote attackers to cause a denial of service via a crafted HTTP response, related to Vary headers.
CVE-2016-3951	Double free vulnerability in drivers/net/usb/cdc_ncm.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (system crash) or possibly have unspecified other impact by inserting a USB device with an invalid USB descriptor.
CVE-2016-3955	The usbip_recv_xbuff function in drivers/usb/usbip/usbip_common.c in the Linux kernel before 4.5.3 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via a crafted length value in a USB/IP packet.
CVE-2016-3961	Xen and the Linux kernel through 4.5.x do not properly suppress hugetlbfs support in x86 PV guests, which allows local PV guest OS users to cause a denial of service (guest OS crash) by attempting to access a hugetlbfs mapped area.
CVE-2016-3990	Heap-based buffer overflow in the horizontalDifference8 function in tif_pixarlog.c in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted TIFF image to tiffcp.
CVE-2016-3991	Heap-based buffer overflow in the loadImage function in the tiffcrop tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted TIFF image with zero tiles.
CVE-2016-3993	Off-by-one error in the __imlib_MergeUpdate function in lib/updates.c in imlib2 before 1.4.9 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via crafted coordinates.
CVE-2016-3994	The GIF loader in imlib2 before 1.4.9 allows remote attackers to cause a denial of service (application crash) or obtain sensitive information via a crafted image, which triggers an out-of-bounds read.
CVE-2016-4001	Buffer overflow in the stellaris_enet_receive function in hw/net/stellaris_enet.c in QEMU, when the Stellaris ethernet controller is configured to accept large packets, allows remote attackers to cause a denial of service (QEMU crash) via a large packet.
CVE-2016-4002	Buffer overflow in the mipsnet_receive function in hw/net/mipsnet.c in QEMU, when the guest NIC is configured to accept large packets, allows remote attackers to cause a denial of service (memory

	corruption and QEMU crash) or possibly execute arbitrary code via a packet larger than 1514 bytes.
CVE-2016-4008	The _asn1_extract_der_octet function in lib/decoding.c in GNU Libtasn1 before 4.8, when used without the ASN1_DECODE_FLAG_STRICT_DER flag, allows remote attackers to cause a denial of service (infinite recursion) via a crafted certificate.
CVE-2016-4020	The patch_instruction function in hw/i386/kvmvapic.c in QEMU does not initialize the imm32 variable, which allows local guest OS administrators to obtain sensitive information from host stack memory by accessing the Task Priority Register (TPR).
CVE-2016-4024	Integer overflow in imlib2 before 1.4.9 on 32-bit platforms allows remote attackers to execute arbitrary code via large dimensions in an image, which triggers an out-of-bounds heap memory write operation.
CVE-2016-4036	The quagga package before 0.99.23-2.6.1 in openSUSE and SUSE Linux Enterprise Server 11 SP 1 uses weak permissions for /etc/quagga, which allows local users to obtain sensitive information by reading files in the directory.
CVE-2016-4037	The ehci_advance_state function in hw/usb/hcd-ehci.c in QEMU allows local guest OS administrators to cause a denial of service (infinite loop and CPU consumption) via a circular split isochronous transfer descriptor (siTD) list, a related issue to CVE-2015-8558.
CVE-2016-4049	The bgp_dump_routes_func function in bgpd/bgp_dump.c in Quagga does not perform size checks when dumping data, which might allow remote attackers to cause a denial of service (assertion failure and daemon crash) via a large BGP packet.
CVE-2016-4051	Buffer overflow in cachemgr.cgi in Squid 2.x, 3.x before 3.5.17, and 4.x before 4.0.9 might allow remote attackers to cause a denial of service or execute arbitrary code by seeding manager reports with crafted data.
CVE-2016-4052	Multiple stack-based buffer overflows in Squid 3.x before 3.5.17 and 4.x before 4.0.9 allow remote HTTP servers to cause a denial of service or execute arbitrary code via crafted Edge Side Includes (ESI) responses.
CVE-2016-4053	Squid 3.x before 3.5.17 and 4.x before 4.0.9 allow remote attackers to obtain sensitive stack layout information via crafted Edge Side Includes (ESI) responses, related to incorrect use of assert and compiler optimization.
CVE-2016-4054	Buffer overflow in Squid 3.x before 3.5.17 and 4.x before 4.0.9 allows remote attackers to execute arbitrary code via crafted Edge Side Includes (ESI) responses.

CVE-2016-4070	** DISPUTED ** Integer overflow in the php_raw_url_encode function in ext/standard/url.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to cause a denial of service (application crash) via a long string to the rawurlencode function. NOTE: the vendor says "Not sure if this qualifies as security issue (probably not)."
CVE-2016-4071	Format string vulnerability in the php_snmp_error function in ext/snmp/snmp.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to execute arbitrary code via format string specifiers in an SNMP::get call.
CVE-2016-4072	The Phar extension in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allows remote attackers to execute arbitrary code via a crafted filename, as demonstrated by mishandling of \0 characters by the phar_analyze_path function in ext/phar/phar.c.
CVE-2016-4073	Multiple integer overflows in the mbfl_strcut function in ext/mbstring/libmbfl/mbfl/mbfilter.c in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5 allow remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted mb_strcut call.
CVE-2016-4108	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4109	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4110	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4111	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-064.
CVE-2016-4112	Unspecified vulnerability in Adobe Flash Player 21.0.0.213 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11

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

	CVE-2016-1109, CVE-2016-1110, CVE-2016-4108, and CVE-2016-4110.
CVE-2016-4122	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4123	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4124	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4125	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4127	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4128	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4129	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4130	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.

CVE-2016-4131	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4132	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4133	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4134	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4135	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4136	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4137	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4138	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash libraries in Microsoft Internet Explorer 10 and 11 and Microsoft Edge, has unknown impact and attack vectors, a different vulnerability than other CVEs listed in MS16-083.
CVE-2016-4139	Unspecified vulnerability in Adobe Flash Player 21.0.0.242 and earlier, as used in the Adobe Flash

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

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

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

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

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

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

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

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

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

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

	CVE-2016-4219, CVE-2016-4220, CVE-2016-4233, CVE-2016-4234, CVE-2016-4235, CVE-2016-4236, CVE-2016-4237, CVE-2016-4238, CVE-2016-4239, CVE-2016-4240, CVE-2016-4241, CVE-2016-4242, CVE-2016-4243, CVE-2016-4244, CVE-2016-4245, and CVE-2016-4246.
CVE-2016-4222	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4226, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4223	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2016-4224 and CVE-2016-4225.
CVE-2016-4224	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2016-4223 and CVE-2016-4225.
CVE-2016-4225	Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code by leveraging an unspecified "type confusion," a different vulnerability than CVE-2016-4223 and CVE-2016-4224.
CVE-2016-4226	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4227, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.
CVE-2016-4227	Use-after-free vulnerability in Adobe Flash Player before 18.0.0.366 and 19.x through 22.x before 22.0.0.209 on Windows and OS X and before 11.2.202.632 on Linux allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4173, CVE-2016-4174, CVE-2016-4222, CVE-2016-4226, CVE-2016-4228, CVE-2016-4229, CVE-2016-4230, CVE-2016-4231, and CVE-2016-4248.

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

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

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

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

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

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

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

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

	(memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4285, CVE-2016-6922, and CVE-2016-6924.
CVE-2016-4285	Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4274, CVE-2016-4275, CVE-2016-4276, CVE-2016-4280, CVE-2016-4281, CVE-2016-4282, CVE-2016-4283, CVE-2016-4284, CVE-2016-6922, and CVE-2016-6924.
CVE-2016-4286	Adobe Flash Player before 18.0.0.382 and 19.x through 23.x before 23.0.0.185 on Windows and OS X and before 11.2.202.637 on Linux allows attackers to bypass intended access restrictions via unspecified vectors.
CVE-2016-4287	Integer overflow in Adobe Flash Player before 18.0.0.375 and 19.x through 23.x before 23.0.0.162 on Windows and OS X and before 11.2.202.635 on Linux allows attackers to execute arbitrary code via unspecified vectors.
CVE-2016-4300	Integer overflow in the read_SubStreamsInfo function in archive_read_support_format_7zip.c in libarchive before 3.2.1 allows remote attackers to execute arbitrary code via a 7zip file with a large number of substreams, which triggers a heap-based buffer overflow.
CVE-2016-4302	Heap-based buffer overflow in the parse_codes function in archive_read_support_format_rar.c in libarchive before 3.2.1 allows remote attackers to execute arbitrary code via a RAR file with a zero-sized dictionary.
CVE-2016-4324	Use-after-free vulnerability in LibreOffice before 5.1.4 allows remote attackers to execute arbitrary code via a crafted RTF file, related to stylesheet and superscript tokens.
CVE-2016-4429	Stack-based buffer overflow in the clntudp_call function in sunrpc/clnt_udp.c in the GNU C Library (aka glibc or libc6) allows remote servers to cause a denial of service (crash) or possibly unspecified other impact via a flood of crafted ICMP and UDP packets.
CVE-2016-4439	The esp_reg_write function in hw/scsi/esp.c in the 53C9X Fast SCSI Controller (FSC) support in QEMU does not properly check command buffer length, which allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process

	crash) or potentially execute arbitrary code on the QEMU host via unspecified vectors.
CVE-2016-4441	The get_cmd function in hw/scsi/esp.c in the 53C9X Fast SCSI Controller (FSC) support in QEMU does not properly check DMA length, which allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) via unspecified vectors, involving an SCSI command.
CVE-2016-4447	The xmlParseElementDecl function in parser.c in libxml2 before 2.9.4 allows context-dependent attackers to cause a denial of service (heap-based buffer underread and application crash) via a crafted file, involving xmlParseName.
CVE-2016-4448	Format string vulnerability in libxml2 before 2.9.4 allows attackers to have unspecified impact via format string specifiers in unknown vectors.
CVE-2016-4449	XML external entity (XXE) vulnerability in the xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.4, when not in validating mode, allows context-dependent attackers to read arbitrary files or cause a denial of service (resource consumption) via unspecified vectors.
CVE-2016-4450	os/unix/ngx_files.c in nginx before 1.10.1 and 1.11.x before 1.11.1 allows remote attackers to cause a denial of service (NULL pointer dereference and worker process crash) via a crafted request, involving writing a client request body to a temporary file.
CVE-2016-4453	The vmsvga_fifo_run function in hw/display/vmware_vga.c in QEMU allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via a VGA command.
CVE-2016-4454	The vmsvga_fifo_read_raw function in hw/display/vmware_vga.c in QEMU allows local guest OS administrators to obtain sensitive host memory information or cause a denial of service (QEMU process crash) by changing FIFO registers and issuing a VGA command, which triggers an out-of-bounds read.
CVE-2016-4470	The key_reject_and_link function in security/keys/key.c in the Linux kernel through 4.6.3 does not ensure that a certain data structure is initialized, which allows local users to cause a denial of service (system crash) via vectors involving a crafted keyctl request2 command.
CVE-2016-4476	hostapd 0.6.7 through 2.5 and wpa_supplicant 0.6.7 through 2.5 do not reject \n and \r characters in passphrase parameters, which allows remote attackers to cause a denial of service (daemon outage) via a crafted WPS operation.
CVE-2016-4477	wpa_supplicant 0.4.0 through 2.5 does not reject \n and \r characters in passphrase parameters, which

	allows local users to trigger arbitrary library loading and consequently gain privileges, or cause a denial of service (daemon outage), via a crafted (1) SET, (2) SET_CRED, or (3) SET_NETWORK command.
CVE-2016-4482	The proc_connectinfo function in drivers/usb/core/devio.c in the Linux kernel through 4.6 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted USBDEVFS_CONNECTINFO ioctl call.
CVE-2016-4483	The xmlBufAttrSerializeTxtContent function in xmlsave.c in libxml2 allows context-dependent attackers to cause a denial of service (out-of-bounds read and application crash) via a non-UTF-8 attribute value, related to serialization. NOTE: this vulnerability may be a duplicate of CVE-2016-3627.
CVE-2016-4484	The Debian initrd script for the cryptsetup package 2:1.7.3-2 and earlier allows physically proximate attackers to gain shell access via many log in attempts with an invalid password.
CVE-2016-4485	The llc_cmsg_rcv function in net/llc/af_llc.c in the Linux kernel before 4.5.5 does not initialize a certain data structure, which allows attackers to obtain sensitive information from kernel stack memory by reading a message.
CVE-2016-4486	The rtnl_fill_link_ifmap function in net/core/rtnetlink.c in the Linux kernel before 4.5.5 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory by reading a Netlink message.
CVE-2016-4487	Use-after-free vulnerability in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary, related to "btypevec."
CVE-2016-4488	Use-after-free vulnerability in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary, related to "ktypevec."
CVE-2016-4489	Integer overflow in the gnu_special function in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary, related to the "demangling of virtual tables."
CVE-2016-4490	Integer overflow in cp-demangle.c in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary, related to inconsistent use of the long and int types for lengths.
CVE-2016-4491	The d_print_comp function in cp-demangle.c in libiberty allows remote attackers to cause a denial of service

	(segmentation fault and crash) via a crafted binary, which triggers infinite recursion and a buffer overflow, related to a node having "itself as ancestor more than once."
CVE-2016-4492	Buffer overflow in the do_type function in cplus-dem.c in libiberty allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted binary.
CVE-2016-4493	The demangle_template_value_parm and do_hpacc_template_literal functions in cplus-dem.c in libiberty allow remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted binary.
CVE-2016-4537	The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 accepts a negative integer for the scale argument, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call.
CVE-2016-4538	The bcpowmod function in ext/bcmath/bcmath.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 modifies certain data structures without considering whether they are copies of the _zero_, _one_, or _two_ global variable, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted call.
CVE-2016-4539	The xml_parse_into_struct function in ext/xml/xml.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (buffer under-read and segmentation fault) or possibly have unspecified other impact via crafted XML data in the second argument, leading to a parser level of zero.
CVE-2016-4540	The grapheme_stripos function in ext/intl/grapheme/grapheme_string.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a negative offset.
CVE-2016-4541	The grapheme_strpos function in ext/intl/grapheme/grapheme_string.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a negative offset.
CVE-2016-4542	The exif_process_IFD_TAG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not properly construct spprintf arguments, which allows remote attackers to cause a

	denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.
CVE-2016-4543	The exif_process_IFD_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate IFD sizes, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.
CVE-2016-4544	The exif_process_TIFF_in_JPEG function in ext/exif/exif.c in PHP before 5.5.35, 5.6.x before 5.6.21, and 7.x before 7.0.6 does not validate TIFF start data, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via crafted header data.
CVE-2016-4553	client_side.cc in Squid before 3.5.18 and 4.x before 4.0.10 does not properly ignore the Host header when absolute-URI is provided, which allows remote attackers to conduct cache-poisoning attacks via an HTTP request.
CVE-2016-4554	mime_header.cc in Squid before 3.5.18 allows remote attackers to bypass intended same-origin restrictions and possibly conduct cache-poisoning attacks via a crafted HTTP Host header, aka a "header smuggling" issue.
CVE-2016-4555	client_side_request.cc in Squid 3.x before 3.5.18 and 4.x before 4.0.10 allows remote servers to cause a denial of service (crash) via crafted Edge Side Includes (ESI) responses.
CVE-2016-4556	Double free vulnerability in Esi.cc in Squid 3.x before 3.5.18 and 4.x before 4.0.10 allows remote servers to cause a denial of service (crash) via a crafted Edge Side Includes (ESI) response.
CVE-2016-4557	The replace_map_fd_with_map_ptr function in kernel/bpf/verifier.c in the Linux kernel before 4.5.5 does not properly maintain an fd data structure, which allows local users to gain privileges or cause a denial of service (use-after-free) via crafted BPF instructions that reference an incorrect file descriptor.
CVE-2016-4558	The BPF subsystem in the Linux kernel before 4.5.5 mishandles reference counts, which allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted application on (1) a system with more than 32 Gb of memory, related to the program reference count or (2) a 1 Tb system, related to the map reference count.
CVE-2016-4565	The InfiniBand (aka IB) stack in the Linux kernel before 4.5.3 incorrectly relies on the write system call, which allows local users to cause a denial of service (kernel memory write operation) or possibly have unspecified other impact via a uAPI interface.

CVE-2016-4568	drivers/media/v4l2-core/videobuf2-v4l2.c in the Linux kernel before 4.5.3 allows local users to cause a denial of service (kernel memory write operation) or possibly have unspecified other impact via a crafted number of planes in a VIDIOC_DQBUF ioctl call.
CVE-2016-4569	The snd_timer_user_params function in sound/core/timer.c in the Linux kernel through 4.6 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via crafted use of the ALSA timer interface.
CVE-2016-4574	Off-by-one error in the append_utf8_value function in the DN decoder (dn.c) in Libksba before 1.3.4 allows remote attackers to cause a denial of service (out-of-bounds read) via invalid utf-8 encoded data. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-4356.
CVE-2016-4578	sound/core/timer.c in the Linux kernel through 4.6 does not initialize certain r1 data structures, which allows local users to obtain sensitive information from kernel stack memory via crafted use of the ALSA timer interface, related to the (1) snd_timer_user_ccallback and (2) snd_timer_user_tinterrupt functions.
CVE-2016-4579	Libksba before 1.3.4 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via unspecified vectors, related to the "returned length of the object from _ksba_ber_parse_tl."
CVE-2016-4580	The x25_negotiate_facilities function in net/x25/x25_facilities.c in the Linux kernel before 4.5.5 does not properly initialize a certain data structure, which allows attackers to obtain sensitive information from kernel stack memory via an X.25 Call Request.
CVE-2016-4581	fs/pnode.c in the Linux kernel before 4.5.4 does not properly traverse a mount propagation tree in a certain case involving a slave mount, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted series of mount system calls.
CVE-2016-4583	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to bypass the Same Origin Policy and obtain image date from an unintended web site via a timing attack involving an SVG document.
CVE-2016-4585	Cross-site scripting (XSS) vulnerability in the WebKit Page Loading implementation in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to inject arbitrary web script or HTML via an HTTP response specifying redirection that is mishandled by Safari.
CVE-2016-4586	WebKit in Apple Safari before 9.1.2 and tvOS before 9.2.2 allows remote attackers to execute arbitrary code

	or cause a denial of service (memory corruption) via a crafted web site.
CVE-2016-4588	WebKit in Apple tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.
CVE-2016-4589	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4622, CVE-2016-4623, and CVE-2016-4624.
CVE-2016-4590	WebKit in Apple iOS before 9.3.3 and Safari before 9.1.2 mishandles about: URLs, which allows remote attackers to bypass the Same Origin Policy via a crafted web site.
CVE-2016-4591	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 mishandles the location variable, which allows remote attackers to access the local filesystem via unspecified vectors.
CVE-2016-4613	An issue was discovered in certain Apple products. Safari before 10.0.1 is affected. iCloud before 6.0.1 is affected. iTunes before 12.5.2 is affected. tvOS before 10.0.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive information via a crafted web site.
CVE-2016-4622	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4589, CVE-2016-4623, and CVE-2016-4624.
CVE-2016-4623	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4589, CVE-2016-4622, and CVE-2016-4624.
CVE-2016-4624	WebKit in Apple iOS before 9.3.3, Safari before 9.1.2, and tvOS before 9.2.2 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4589, CVE-2016-4622, and CVE-2016-4623.
CVE-2016-4651	Cross-site scripting (XSS) vulnerability in the WebKit JavaScript bindings in Apple iOS before 9.3.3 and Safari before 9.1.2 allows remote attackers to inject arbitrary web script or HTML via a crafted HTTP/0.9 response, related to a "cross-protocol cross-site scripting (XPXSS)" vulnerability.

CVE-2016-4657	WebKit in Apple iOS before 9.3.5 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.
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-2016-4666	An issue was discovered in certain Apple products. iOS before 10.1 is affected. Safari before 10.0.1 is affected. tvOS before 10.0.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2016-4707	CFNetwork in Apple iOS before 10 and OS X before 10.12 mishandles Local Storage deletion, which allows local users to discover the visited web sites of arbitrary users via unspecified vectors.
CVE-2016-4728	WebKit in Apple iOS before 10, tvOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10 mishandles error prototypes, which allows remote attackers to execute arbitrary code via a crafted web site.
CVE-2016-4733	WebKit in Apple iOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4730, CVE-2016-4734, and CVE-2016-4735.
CVE-2016-4734	WebKit in Apple iOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4730, CVE-2016-4733, and CVE-2016-4735.
CVE-2016-4735	WebKit in Apple iOS before 10, Safari before 10, and tvOS before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4611, CVE-2016-4730, CVE-2016-4733, and CVE-2016-4734.
CVE-2016-4738	libxslt in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.
CVE-2016-4759	WebKit in Apple iOS before 10, tvOS before 10, iTunes before 12.5.1 on Windows, and Safari before

	10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4765, CVE-2016-4766, CVE-2016-4767, and CVE-2016-4768.
CVE-2016-4760	WebKit in Apple iOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10 allows remote attackers to conduct DNS rebinding attacks against non-HTTP Safari sessions by leveraging HTTP/0.9 support.
CVE-2016-4762	WebKit in Apple iOS before 10, iTunes before 12.5.1 on Windows, iCloud before 6.0 on Windows, and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site.
CVE-2016-4764	An issue was discovered in certain Apple products. iOS before 10 is affected. Safari before 10 is affected. iTunes before 12.5.1 is affected. tvOS before 10 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2016-4765	WebKit in Apple iOS before 10, tvOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4759, CVE-2016-4766, CVE-2016-4767, and CVE-2016-4768.
CVE-2016-4767	WebKit in Apple iOS before 10, tvOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4759, CVE-2016-4765, CVE-2016-4766, and CVE-2016-4768.
CVE-2016-4768	WebKit in Apple iOS before 10, tvOS before 10, iTunes before 12.5.1 on Windows, and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, a different vulnerability than CVE-2016-4759, CVE-2016-4765, CVE-2016-4766, and CVE-2016-4767.
CVE-2016-4769	WebKit in Apple iTunes before 12.5.1 on Windows and Safari before 10 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2016-4794	Use-after-free vulnerability in mm/percpu.c in the Linux kernel through 4.6 allows local users to cause a denial of service (BUG) or possibly have unspecified other

	impact via crafted use of the mmap and bpf system calls.
CVE-2016-4804	The read_boot function in boot.c in dosfstools before 4.0 allows attackers to cause a denial of service (crash) via a crafted filesystem, which triggers a heap-based buffer overflow in the (1) read_fat function or an out-of-bounds heap read in (2) get_fat function.
CVE-2016-4809	The archive_read_format_cpio_read_header function in archive_read_support_format_cpio.c in libarchive before 3.2.1 allows remote attackers to cause a denial of service (application crash) via a CPIO archive with a large symlink.
CVE-2016-4913	The get_rock_ridge_filename function in fs/isofs/rock.c in the Linux kernel before 4.5.5 mishandles NM (aka alternate name) entries containing \0 characters, which allows local users to obtain sensitive information from kernel memory or possibly have unspecified other impact via a crafted isofs filesystem.
CVE-2016-4951	The tipc_nl_publ_dump function in net/tipc/socket.c in the Linux kernel through 4.6 does not verify socket existence, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a dumpit operation.
CVE-2016-4952	QEMU (aka Quick Emulator), when built with VMWARE PVSCSI paravirtual SCSI bus emulation support, allows local guest OS administrators to cause a denial of service (out-of-bounds array access) via vectors related to the (1) PVSCSI_CMD_SETUP_RINGS or (2) PVSCSI_CMD_SETUP_MSG_RING SCSI command.
CVE-2016-4954	The process_packet function in ntp_proto.c in ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (peer-variable modification) by sending spoofed packets from many source IP addresses in a certain scenario, as demonstrated by triggering an incorrect leap indication.
CVE-2016-4955	ntpd in NTP 4.x before 4.2.8p8, when autokey is enabled, allows remote attackers to cause a denial of service (peer-variable clearing and association outage) by sending (1) a spoofed crypto-NAK packet or (2) a packet with an incorrect MAC value at a certain time.
CVE-2016-4956	ntpd in NTP 4.x before 4.2.8p8 allows remote attackers to cause a denial of service (interleaved-mode transition and time change) via a spoofed broadcast packet. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-1548.
CVE-2016-4971	GNU wget before 1.18 allows remote servers to write to arbitrary files by redirecting a request from HTTP to a crafted FTP resource.

CVE-2016-4997	The compat IPT_SO_SET_REPLACE and IP6T_SO_SET_REPLACE setsockopt implementations in the netfilter subsystem in the Linux kernel before 4.6.3 allow local users to gain privileges or cause a denial of service (memory corruption) by leveraging in-container root access to provide a crafted offset value that triggers an unintended decrement.
CVE-2016-4998	The IPT_SO_SET_REPLACE setsockopt implementation in the netfilter subsystem in the Linux kernel before 4.6 allows local users to cause a denial of service (out-of-bounds read) or possibly obtain sensitive information from kernel heap memory by leveraging in-container root access to provide a crafted offset value that leads to crossing a ruleset blob boundary.
CVE-2016-5008	libvirt before 2.0.0 improperly disables password checking when the password on a VNC server is set to an empty string, which allows remote attackers to bypass authentication and establish a VNC session by connecting to the server.
CVE-2016-5018	In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 a malicious web application was able to bypass a configured SecurityManager via a Tomcat utility method that was accessible to web applications.
CVE-2016-5102	Buffer overflow in the readgifimage function in gif2tiff.c in the gif2tiff tool in LibTIFF 4.0.6 allows remote attackers to cause a denial of service (segmentation fault) via a crafted gif file.
CVE-2016-5104	The socket_create function in common/socket.c in libimobiledevice and libusbmuxd allows remote attackers to bypass intended access restrictions and communicate with services on iOS devices by connecting to an IPv4 TCP socket.
CVE-2016-5105	The megasas_dcmd_cfg_read function in hw/scsi/megasas.c in QEMU, when built with MegaRAID SAS 8708EM2 Host Bus Adapter emulation support, uses an uninitialized variable, which allows local guest administrators to read host memory via vectors involving a MegaRAID Firmware Interface (MFI) command.
CVE-2016-5106	The megasas_dcmd_set_properties function in hw/scsi/megasas.c in QEMU, when built with MegaRAID SAS 8708EM2 Host Bus Adapter emulation support, allows local guest administrators to cause a denial of service (out-of-bounds write access) via vectors involving a MegaRAID Firmware Interface (MFI) command.
CVE-2016-5107	The megasas_lookup_frame function in QEMU, when built with MegaRAID SAS 8708EM2 Host Bus Adapter emulation support, allows local guest OS administrators

	to cause a denial of service (out-of-bounds read and crash) via unspecified vectors.
CVE-2016-5116	gd_xbm.c in the GD Graphics Library (aka libgd) before 2.2.0, as used in certain custom PHP 5.5.x configurations, allows context-dependent attackers to obtain sensitive information from process memory or cause a denial of service (stack-based buffer under-read and application crash) via a long name.
CVE-2016-5118	The OpenBlob function in blob.c in GraphicsMagick before 1.3.24 and ImageMagick allows remote attackers to execute arbitrary code via a l (pipe) character at the start of a filename.
CVE-2016-5126	Heap-based buffer overflow in the iscsi_aio_ioctl function in block/iscsi.c in QEMU allows local guest OS users to cause a denial of service (QEMU process crash) or possibly execute arbitrary code via a crafted iSCSI asynchronous I/O ioctl call.
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-2016-5180	Heap-based buffer overflow in the ares_create_query function in c-ares 1.x before 1.12.0 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly execute arbitrary code via a hostname with an escaped trailing dot.
CVE-2016-5181	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android permitted execution of v8 microtasks while the DOM was in an inconsistent state, which allowed a remote

	attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages.
CVE-2016-5182	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android had insufficient validation in bitmap handling, which allowed a remote attacker to potentially exploit heap corruption via crafted HTML pages.
CVE-2016-5183	A heap use after free in PDFium in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android allows a remote attacker to potentially exploit heap corruption via crafted PDF files.
CVE-2016-5184	PDFium in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object lifecycles in CFFL_FormFillter::KillFocusForAnnot, which allowed a remote attacker to potentially exploit heap corruption via crafted PDF files.
CVE-2016-5185	Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly allowed reentrance of FrameView::updateLifecyclePhasesInternal(), which allowed a remote attacker to perform an out of bounds memory read via crafted HTML pages.
CVE-2016-5186	Devtools in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled objects after a tab crash, which allowed a remote attacker to perform an out of bounds memory read via crafted PDF files.
CVE-2016-5187	Google Chrome prior to 54.0.2840.85 for Android incorrectly handled rapid transition into and out of full screen mode, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages.
CVE-2016-5188	Multiple issues in Blink in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux allow a remote attacker to spoof various parts of browser UI via crafted HTML pages.
CVE-2016-5189	Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android permitted navigation to blob URLs with non-canonical origins, which allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via crafted HTML pages.
CVE-2016-5190	Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux; 54.0.2840.85 for Android incorrectly handled object lifecycles during shutdown, which allowed a remote attacker to perform an out of bounds memory read via crafted HTML pages.
CVE-2016-5191	Bookmark handling in Google Chrome prior to 54.0.2840.59 for Windows, Mac, and Linux;

	54.0.2840.85 for Android had insufficient validation of supplied data, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via crafted HTML pages, as demonstrated by an interpretation conflict between userinfo and scheme in an http://javascript:payload@example.com URL.
CVE-2016-5192	Blink in Google Chrome prior to 54.0.2840.59 for Windows missed a CORS check on redirect in TextTrackLoader, which allowed a remote attacker to bypass cross-origin restrictions via crafted HTML pages.
CVE-2016-5193	Google Chrome prior to 54.0 for iOS had insufficient validation of URLs for windows open by DOM, which allowed a remote attacker to bypass restrictions on navigation to certain URL schemes via crafted HTML pages.
CVE-2016-5194	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-5195	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exploited in the wild in October 2016, aka "Dirty COW."
CVE-2016-5198	V8 in Google Chrome prior to 54.0.2840.90 for Linux, and 54.0.2840.85 for Android, and 54.0.2840.87 for Windows and Mac included incorrect optimisation assumptions, which allowed a remote attacker to perform arbitrary read/write operations, leading to code execution, via a crafted HTML page.
CVE-2016-5199	An off by one error resulting in an allocation of zero size in FFmpeg in Google Chrome prior to 54.0.2840.98 for Mac, and 54.0.2840.99 for Windows, and 54.0.2840.100 for Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted video file.
CVE-2016-5200	V8 in Google Chrome prior to 54.0.2840.98 for Mac, and 54.0.2840.99 for Windows, and 54.0.2840.100 for Linux, and 55.0.2883.84 for Android incorrectly applied type rules, which allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5201	A leak of privateClass in the extensions API in Google Chrome prior to 54.0.2840.100 for Linux, and 54.0.2840.99 for Windows, and 54.0.2840.98 for Mac allowed a remote attacker to access privileged JavaScript code via a crafted HTML page.

CVE-2016-5202	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-5203	A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2016-5204	Leaking of an SVG shadow tree leading to corruption of the DOM tree in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2016-5205	Blink in Google Chrome prior to 55.0.2883.75 for Linux, Windows and Mac, incorrectly handles deferred page loads, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2016-5206	The PDF plugin in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly followed redirects, which allowed a remote attacker to bypass the Same Origin Policy via a crafted HTML page.
CVE-2016-5207	In Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android, corruption of the DOM tree could occur during the removal of a full screen element, which allowed a remote attacker to achieve arbitrary code execution via a crafted HTML page.
CVE-2016-5208	Blink in Google Chrome prior to 55.0.2883.75 for Linux and Windows, and 55.0.2883.84 for Android allowed possible corruption of the DOM tree during synchronous event handling, which allowed a remote attacker to inject arbitrary scripts or HTML (UXSS) via a crafted HTML page.
CVE-2016-5209	Bad casting in bitmap manipulation in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5210	Heap buffer overflow during TIFF image parsing in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2016-5211	A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and

	55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2016-5212	Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android insufficiently sanitized DevTools URLs, which allowed a remote attacker to read local files via a crafted HTML page.
CVE-2016-5213	A use after free in V8 in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5214	Google Chrome prior to 55.0.2883.75 for Windows mishandled downloaded files, which allowed a remote attacker to prevent the downloaded file from receiving the Mark of the Web via a crafted HTML page.
CVE-2016-5215	A use after free in webaudio in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2016-5216	A use after free in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to perform an out of bounds memory read via a crafted PDF file.
CVE-2016-5217	The extensions API in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly permitted access to privileged plugins, which allowed a remote attacker to bypass site isolation via a crafted HTML page.
CVE-2016-5218	The extensions API in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled navigation within PDFs, which allowed a remote attacker to temporarily spoof the contents of the Omnibox (URL bar) via a crafted HTML page containing PDF data.
CVE-2016-5219	A heap use after free in V8 in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2016-5220	PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled navigation within PDFs, which allowed a remote attacker to read local files via a crafted PDF file.
CVE-2016-5221	Type confusion in libGLESv2 in ANGLE in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android possibly allowed a

	remote attacker to bypass buffer validation via a crafted HTML page.
CVE-2016-5222	Incorrect handling of invalid URLs in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2016-5223	Integer overflow in PDFium in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to potentially exploit heap corruption or DoS via a crafted PDF file.
CVE-2016-5224	A timing attack on denormalized floating point arithmetic in SVG filters in Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android allowed a remote attacker to bypass the Same Origin Policy via a crafted HTML page.
CVE-2016-5225	Blink in Google Chrome prior to 55.0.2883.75 for Mac, Windows and Linux, and 55.0.2883.84 for Android incorrectly handled form actions, which allowed a remote attacker to bypass Content Security Policy via a crafted HTML page.
CVE-2016-5226	Blink in Google Chrome prior to 55.0.2883.75 for Linux, Windows and Mac executed javascript: URLs entered in the URL bar in the context of the current tab, which allowed a socially engineered user to XSS themselves by dragging and dropping a javascript: URL into the URL bar.
CVE-2016-5238	The get_cmd function in hw/scsi/esp.c in QEMU might allow local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) via vectors related to reading from the information transfer buffer in non-DMA mode.
CVE-2016-5243	The tipc_nl_compat_link_dump function in net/tipc/netlink_compat.c in the Linux kernel through 4.6.3 does not properly copy a certain string, which allows local users to obtain sensitive information from kernel stack memory by reading a Netlink message.
CVE-2016-5244	The rds_inc_info_copy function in net/rds/recv.c in the Linux kernel through 4.6.3 does not initialize a certain structure member, which allows remote attackers to obtain sensitive information from kernel stack memory by reading an RDS message.
CVE-2016-5250	Mozilla Firefox before 48.0, Firefox ESR < 45.4 and Thunderbird < 45.4 allow remote attackers to obtain sensitive information about the previously retrieved page via Resource Timing API calls.

CVE-2016-5251	Mozilla Firefox before 48.0 allows remote attackers to spoof the location bar via crafted characters in the media type of a data: URL.
CVE-2016-5252	Stack-based buffer underflow in the mozilla::gfx::BasePoint4d function in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allows remote attackers to execute arbitrary code via crafted two-dimensional graphics data that is mishandled during clipping-region calculations.
CVE-2016-5254	Use-after-free vulnerability in the nsXULPopupManager::KeyDown function in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allows attackers to execute arbitrary code or cause a denial of service (heap memory corruption and application crash) by leveraging keyboard access to use the Alt key during selection of top-level menu items.
CVE-2016-5255	Use-after-free vulnerability in the js::PreliminaryObjectArray::sweep function in Mozilla Firefox before 48.0 allows remote attackers to execute arbitrary code via crafted JavaScript that is mishandled during incremental garbage collection.
CVE-2016-5256	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 49.0 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2016-5257	Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 49.0, Firefox ESR 45.x before 45.4 and Thunderbird < 45.4 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors.
CVE-2016-5258	Use-after-free vulnerability in the WebRTC socket thread in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allows remote attackers to execute arbitrary code by leveraging incorrect free operations on DTLS objects during the shutdown of a WebRTC session.
CVE-2016-5259	Use-after-free vulnerability in the CanonicalizeXPCOMParticipant function in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allows remote attackers to execute arbitrary code via a script that closes its own Service Worker within a nested sync event loop.
CVE-2016-5260	Mozilla Firefox before 48.0 mishandles changes from 'INPUT type="password"' to 'INPUT type="text"' within a single Session Manager session, which might allow attackers to discover cleartext passwords by reading a session restoration file.

CVE-2016-5261	Integer overflow in the WebSocketChannel class in the WebSockets subsystem in Mozilla Firefox before 48.0 and Firefox ESR < 45.4 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted packets that trigger incorrect buffer-resize operations during buffering.
CVE-2016-5262	Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 process JavaScript event-handler attributes of a MARQUEE element within a sandboxed IFRAME element that lacks the sandbox="allow-scripts" attribute value, which makes it easier for remote attackers to conduct cross-site scripting (XSS) attacks via a crafted web site.
CVE-2016-5263	The nsDisplayList::HitTest function in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 mishandles rendering display transformation, which allows remote attackers to execute arbitrary code via a crafted web site that leverages "type confusion."
CVE-2016-5264	Use-after-free vulnerability in the nsNodeUtils::NativeAnonymousChildListChange function in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via an SVG element that is mishandled during effect application.
CVE-2016-5265	Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.3 allow user-assisted remote attackers to bypass the Same Origin Policy, and conduct Universal XSS (UXSS) attacks or read arbitrary files, by arranging for the presence of a crafted HTML document and a crafted shortcut file in the same local directory.
CVE-2016-5266	Mozilla Firefox before 48.0 does not properly restrict drag-and-drop (aka dataTransfer) actions for file: URIs, which allows user-assisted remote attackers to access local files via a crafted web site.
CVE-2016-5268	Mozilla Firefox before 48.0 does not properly set the LINKABLE and URI_SAFE_FOR_UNTRUSTED_CONTENT flags of about: URLs that are used for error pages, which makes it easier for remote attackers to conduct spoofing attacks via a crafted URL, as demonstrated by misleading text after an about:neterror?d= substring.
CVE-2016-5270	Heap-based buffer overflow in the nsCaseTransformTextRunFactory::TransformString function in Mozilla Firefox before 49.0, Firefox ESR 45.x before 45.4, and Thunderbird < 45.4 allows remote attackers to cause a denial of service (boolean out-of-bounds write) or possibly have unspecified other impact via Unicode characters that are mishandled during text conversion.

CVE-2016-5271	The PropertyProvider::GetSpacingInternal function in Mozilla Firefox before 49.0 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via text runs in conjunction with a "display: contents" Cascading Style Sheets (CSS) property.
CVE-2016-5272	The nsImageGeometryMixin class in Mozilla Firefox before 49.0, Firefox ESR 45.x before 45.4, and Thunderbird < 45.4 does not properly perform a cast of an unspecified variable during handling of INPUT elements, which allows remote attackers to execute arbitrary code via a crafted web site.
CVE-2016-5273	The mozilla::a11y::HyperTextAccessible::GetChildOffset function in the accessibility implementation in Mozilla Firefox before 49.0 allows remote attackers to execute arbitrary code via a crafted web site.
CVE-2016-5274	Use-after-free vulnerability in the nsFrameManager::CaptureFrameState function in Mozilla Firefox before 49.0, Firefox ESR 45.x before 45.4, and Thunderbird < 45.4 allows remote attackers to execute arbitrary code by leveraging improper interaction between restyling and the Web Animations model implementation.
CVE-2016-5275	Buffer overflow in the mozilla::gfx::FilterSupport::ComputeSourceNeededRegions function in Mozilla Firefox before 49.0 allows remote attackers to execute arbitrary code by leveraging improper interaction between empty filters and CANVAS element rendering.
CVE-2016-5276	Use-after-free vulnerability in the mozilla::a11y::DocAccessible::ProcessInvalidationList function in Mozilla Firefox before 49.0, Firefox ESR 45.x before 45.4, and Thunderbird < 45.4 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) via an aria-owns attribute.
CVE-2016-5277	Use-after-free vulnerability in the nsRefreshDriver::Tick function in Mozilla Firefox before 49.0, Firefox ESR 45.x before 45.4, and Thunderbird < 45.4 allows remote attackers to execute arbitrary code or cause a denial of service (heap memory corruption) by leveraging improper interaction between timeline destruction and the Web Animations model implementation.
CVE-2016-5278	Heap-based buffer overflow in the nsBMPEncoder::AddImageFrame function in Mozilla Firefox before 49.0, Firefox ESR 45.x before 45.4, and Thunderbird < 45.4 allows remote attackers to execute arbitrary code via a crafted image data that is

	mishandled during the encoding of an image frame to an image.
CVE-2016-5279	Mozilla Firefox before 49.0 allows user-assisted remote attackers to obtain sensitive full-pathname information during a local-file drag-and-drop operation via crafted JavaScript code.
CVE-2016-5280	Use-after-free vulnerability in the mozilla::nsTextNodeDirectionalityMap::RemoveElementFromMap function in Mozilla Firefox before 49.0, Firefox ESR 45.x before 45.4, and Thunderbird < 45.4 allows remote attackers to execute arbitrary code via bidirectional text.
CVE-2016-5281	Use-after-free vulnerability in the DOMSVGLength class in Mozilla Firefox before 49.0, Firefox ESR 45.x before 45.4, and Thunderbird < 45.4 allows remote attackers to execute arbitrary code by leveraging improper interaction between JavaScript code and an SVG document.
CVE-2016-5282	Mozilla Firefox before 49.0 does not properly restrict the scheme in favicon requests, which might allow remote attackers to obtain sensitive information via unspecified vectors, as demonstrated by a jar: URL for a favicon resource.
CVE-2016-5283	Mozilla Firefox before 49.0 allows remote attackers to bypass the Same Origin Policy via a crafted fragment identifier in the SRC attribute of an IFRAME element, leading to insufficient restrictions on link-color information after a document is resized.
CVE-2016-5284	Mozilla Firefox before 49.0, Firefox ESR 45.x before 45.4, and Thunderbird < 45.4 rely on unintended expiration dates for Preloaded Public Key Pinning, which allows man-in-the-middle attackers to spoof add-on updates by leveraging possession of an X.509 server certificate for addons.mozilla.org signed by an arbitrary built-in Certification Authority.
CVE-2016-5285	A NULL pointer dereference flaw was found in the way NSS handled invalid Diffie-Hellman keys. A remote client could use this flaw to crash a TLS/SSL server using NSS.
CVE-2016-5287	A potentially exploitable use-after-free crash during actor destruction with service workers. This issue does not affect releases earlier than Firefox 49. This vulnerability affects Firefox < 49.0.2.
CVE-2016-5288	Web content could access information in the HTTP cache if e10s is disabled. This can reveal some visited URLs and the contents of those pages. This issue affects Firefox 48 and 49. This vulnerability affects Firefox < 49.0.2.
CVE-2016-5289	Memory safety bugs were reported in Firefox 49. 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 < 50.
CVE-2016-5290	Memory safety bugs were reported in Firefox 49 and Firefox ESR 45.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 45.5, Firefox ESR < 45.5, and Firefox < 50.
CVE-2016-5291	A same-origin policy bypass with local shortcut files to load arbitrary local content from disk. This vulnerability affects Thunderbird < 45.5, Firefox ESR < 45.5, and Firefox < 50.
CVE-2016-5292	During URL parsing, a maliciously crafted URL can cause a potentially exploitable crash. This vulnerability affects Firefox < 50.
CVE-2016-5296	A heap-buffer-overflow in Cairo when processing SVG content caused by compiler optimization, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 45.5, Firefox ESR < 45.5, and Firefox < 50.
CVE-2016-5297	An error in argument length checking in JavaScript, leading to potential integer overflows or other bounds checking issues. This vulnerability affects Thunderbird < 45.5, Firefox ESR < 45.5, and Firefox < 50.
CVE-2016-5300	The XML parser in Expat does not use sufficient entropy for hash initialization, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted identifiers in an XML document. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-0876.
CVE-2016-5314	Buffer overflow in the PixarLogDecode function in tif_pixarlog.c in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted TIFF image, as demonstrated by overwriting the vgetparent function pointer with rgb2ycbcr.
CVE-2016-5315	The setByteArray function in tif_dir.c in libtiff 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted tiff image.
CVE-2016-5316	Out-of-bounds read in the PixarLogCleanup function in tif_pixarlog.c in libtiff 4.0.6 and earlier allows remote attackers to crash the application by sending a crafted TIFF image to the rgb2ycbcr tool.
CVE-2016-5317	Buffer overflow in the PixarLogDecode function in libtiff.so in the PixarLogDecode function in libtiff 4.0.6 and earlier, as used in GNOME nautilus, allows

	attackers to cause a denial of service attack (crash) via a crafted TIFF file.
CVE-2016-5318	Stack-based buffer overflow in the _TIFFVGetField function in libtiff 4.0.6 and earlier allows remote attackers to crash the application via a crafted tiff.
CVE-2016-5321	The DumpModeDecode function in libtiff 4.0.6 and earlier allows attackers to cause a denial of service (invalid read and crash) via a crafted tiff image.
CVE-2016-5322	The setByteArray function in tif_dir.c in libtiff 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted tiff image.
CVE-2016-5323	The _TIFFFax3fillruns function in libtiff before 4.0.6 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted Tiff image.
CVE-2016-5337	The megasas_ctrl_get_info function in hw/scsi/megasas.c in QEMU allows local guest OS administrators to obtain sensitive host memory information via vectors related to reading device control information.
CVE-2016-5338	The (1) esp_reg_read and (2) esp_reg_write functions in hw/scsi/esp.c in QEMU allow local guest OS administrators to cause a denial of service (QEMU process crash) or execute arbitrary code on the QEMU host via vectors related to the information transfer buffer.
CVE-2016-5360	HAproxy 1.6.x before 1.6.6, when a deny comes from a reqdeny rule, allows remote attackers to cause a denial of service (uninitialized memory access and crash) or possibly have unspecified other impact via unknown vectors.
CVE-2016-5384	fontconfig before 2.12.1 does not validate offsets, which allows local users to trigger arbitrary free calls and consequently conduct double free attacks and execute arbitrary code via a crafted cache file.
CVE-2016-5385	PHP through 7.0.8 does not attempt to address RFC 3875 section 4.1.18 namespace conflicts and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, as demonstrated by (1) an application that makes a getenv('HTTP_PROXY') call or (2) a CGI configuration of PHP, aka an "httpoxy" issue.
CVE-2016-5387	The Apache HTTP Server through 2.4.23 follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable,

	which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "This mitigation has been assigned the identifier CVE-2016-5387"; in other words, this is not a CVE ID for a vulnerability.
CVE-2016-5388	Apache Tomcat 7.x through 7.0.70 and 8.x through 8.5.4, when the CGI Servlet is enabled, follows RFC 3875 section 4.1.18 and therefore does not protect applications from the presence of untrusted client data in the HTTP_PROXY environment variable, which might allow remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request, aka an "httpoxy" issue. NOTE: the vendor states "A mitigation is planned for future releases of Tomcat, tracked as CVE-2016-5388"; in other words, this is not a CVE ID for a vulnerability.
CVE-2016-5399	The bzread function in ext/bz2/bz2.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted bz2 archive.
CVE-2016-5400	Memory leak in the airspy_probe function in drivers/media/usb/airspy/airspy.c in the airspy USB driver in the Linux kernel before 4.7 allows local users to cause a denial of service (memory consumption) via a crafted USB device that emulates many VFL_TYPE_SDR or VFL_TYPE_SUBDEV devices and performs many connect and disconnect operations.
CVE-2016-5403	The virtqueue_pop function in hw/virtio/virtio.c in QEMU allows local guest OS administrators to cause a denial of service (memory consumption and QEMU process crash) by submitting requests without waiting for completion.
CVE-2016-5412	arch/powerpc/kvm/book3s_hv_rmhandlers.S in the Linux kernel through 4.7 on PowerPC platforms, when CONFIG_KVM_BOOK3S_64_HV is enabled, allows guest OS users to cause a denial of service (host OS infinite loop) by making a H_CEDE hypercall during the existence of a suspended transaction.
CVE-2016-5417	Memory leak in the __res_vinit function in the IPv6 name server management code in libresolv in GNU C Library (aka glibc or libc6) before 2.24 allows remote attackers to cause a denial of service (memory consumption) by leveraging partial initialization of internal resolver data structures.
CVE-2016-5418	The sandboxing code in libarchive 3.2.0 and earlier mishandles hardlink archive entries of non-zero data

	size, which might allow remote attackers to write to arbitrary files via a crafted archive file.
CVE-2016-5419	curl and libcurl before 7.50.1 do not prevent TLS session resumption when the client certificate has changed, which allows remote attackers to bypass intended restrictions by resuming a session.
CVE-2016-5420	curl and libcurl before 7.50.1 do not check the client certificate when choosing the TLS connection to reuse, which might allow remote attackers to hijack the authentication of the connection by leveraging a previously created connection with a different client certificate.
CVE-2016-5421	Use-after-free vulnerability in libcurl before 7.50.1 allows attackers to control which connection is used or possibly have unspecified other impact via unknown vectors.
CVE-2016-5423	PostgreSQL before 9.1.23, 9.2.x before 9.2.18, 9.3.x before 9.3.14, 9.4.x before 9.4.9, and 9.5.x before 9.5.4 allow remote authenticated users to cause a denial of service (NULL pointer dereference and server crash), obtain sensitive memory information, or possibly execute arbitrary code via (1) a CASE expression within the test value subexpression of another CASE or (2) inlining of an SQL function that implements the equality operator used for a CASE expression involving values of different types.
CVE-2016-5424	PostgreSQL before 9.1.23, 9.2.x before 9.2.18, 9.3.x before 9.3.14, 9.4.x before 9.4.9, and 9.5.x before 9.5.4 might allow remote authenticated users with the CREATEDB or CREATEROLE role to gain superuser privileges via a (1) " (double quote), (2) \ (backslash), (3) carriage return, or (4) newline character in a (a) database or (b) role name that is mishandled during an administrative operation.
CVE-2016-5436	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: InnoDB.
CVE-2016-5437	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Log.
CVE-2016-5439	Unspecified vulnerability in Oracle MySQL 5.6.30 and earlier and 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Privileges.
CVE-2016-5440	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows remote administrators to affect availability via vectors related to Server: RBR.

CVE-2016-5441	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Replication.
CVE-2016-5442	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows remote administrators to affect availability via vectors related to Server: Security: Encryption.
CVE-2016-5443	Unspecified vulnerability in Oracle MySQL 5.7.12 and earlier allows local users to affect availability via vectors related to Server: Connection.
CVE-2016-5542	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect integrity via vectors related to Libraries.
CVE-2016-5546	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS v3.0 Base Score 7.5 (Integrity impacts).
CVE-2016-5547	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets,

	such as through a web service. CVSS v3.0 Base Score 5.3 (Availability impacts).
CVE-2016-5548	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS v3.0 Base Score 6.5 (Confidentiality impacts).
CVE-2016-5549	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u121 and 8u112; Java SE Embedded: 8u111. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS v3.0 Base Score 6.5 (Confidentiality impacts).
CVE-2016-5552	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit.

	Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS v3.0 Base Score 5.3 (Integrity impacts).
CVE-2016-5554	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect integrity via vectors related to JMX.
CVE-2016-5573	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot, a different vulnerability than CVE-2016-5582.
CVE-2016-5582	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Hotspot, a different vulnerability than CVE-2016-5573.
CVE-2016-5584	Unspecified vulnerability in Oracle MySQL 5.5.52 and earlier, 5.6.33 and earlier, and 5.7.15 and earlier allows remote administrators to affect confidentiality via vectors related to Server: Security: Encryption.
CVE-2016-5597	Unspecified vulnerability in Oracle Java SE 6u121, 7u111, 8u102; and Java SE Embedded 8u101 allows remote attackers to affect confidentiality via vectors related to Networking.
CVE-2016-5636	Integer overflow in the get_data function in zipimport.c in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 allows remote attackers to have unspecified impact via a negative data size value, which triggers a heap-based buffer overflow.
CVE-2016-5652	An exploitable heap-based buffer overflow exists in the handling of TIFF images in LibTIFF's TIFF2PDF tool. A crafted TIFF document can lead to a heap-based buffer overflow resulting in remote code execution. Vulnerability can be triggered via a saved TIFF file delivered by other means.
CVE-2016-5696	net/ipv4/tcp_input.c in the Linux kernel before 4.7 does not properly determine the rate of challenge ACK segments, which makes it easier for remote attackers to hijack TCP sessions via a blind in-window attack.
CVE-2016-5699	CRLF injection vulnerability in the HTTPConnection.putheader function in urllib2 and urllib

	in CPython (aka Python) before 2.7.10 and 3.x before 3.4.4 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in a URL.
CVE-2016-5728	Race condition in the vop_ioctl function in drivers/misc/mic/vop/vop_vringh.c in the MIC VOP driver in the Linux kernel before 4.6.1 allows local users to obtain sensitive information from kernel memory or cause a denial of service (memory corruption and system crash) by changing a certain header, aka a "double fetch" vulnerability.
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-2016-5828	The start_thread function in arch/powerpc/kernel/process.c in the Linux kernel through 4.6.3 on powerpc platforms mishandles transactional state, which allows local users to cause a denial of service (invalid process state or TM Bad Thing exception, and system crash) or possibly have unspecified other impact by starting and suspending a transaction before an exec system call.
CVE-2016-5829	Multiple heap-based buffer overflows in the hiddev_ioctl_usage function in drivers/hid/usbhid/hiddev.c in the Linux kernel through 4.6.3 allow local users to cause a denial of service or possibly have unspecified other impact via a crafted (1) HIDIOCGUSAGES or (2) HIDIOCSUSAGES ioctl call.
CVE-2016-5844	Integer overflow in the ISO parser in libarchive before 3.2.1 allows remote attackers to cause a denial of service (application crash) via a crafted ISO file.
CVE-2016-6128	The gdImageCropThreshold function in gd_crop.c in the GD Graphics Library (aka libgd) before 2.2.3, as used in PHP before 7.0.9, allows remote attackers to cause a denial of service (application crash) via an invalid color index.
CVE-2016-6130	Race condition in the sclp_ctl_ioctl_sccb function in drivers/s390/char/sclp_ctl.c in the Linux kernel before 4.6 allows local users to obtain sensitive information from kernel memory by changing a certain length value, aka a "double fetch" vulnerability.
CVE-2016-6131	The demangler in GNU Libiberty allows remote attackers to cause a denial of service (infinite loop, stack overflow, and crash) via a cycle in the references of remembered mangled types.
CVE-2016-6132	The gdImageCreateFromTgaCtx function in the GD Graphics Library (aka libgd) before 2.2.3 allows remote

	attackers to cause a denial of service (out-of-bounds read) via a crafted TGA file.
CVE-2016-6136	Race condition in the audit_log_single_execve_arg function in kernel/auditsc.c in the Linux kernel through 4.7 allows local users to bypass intended character-set restrictions or disrupt system-call auditing by changing a certain string, aka a "double fetch" vulnerability.
CVE-2016-6156	Race condition in the ec_device_ioctl_xcmd function in drivers/platform/chrome/cros_ec_dev.c in the Linux kernel before 4.7 allows local users to cause a denial of service (out-of-bounds array access) by changing a certain size value, aka a "double fetch" vulnerability.
CVE-2016-6161	The output function in gd_gif_out.c in the GD Graphics Library (aka libgd) allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted image.
CVE-2016-6185	The XSLoader::load method in XSLoader in Perl does not properly locate .so files when called in a string eval, which might allow local users to execute arbitrary code via a Trojan horse library under the current working directory.
CVE-2016-6186	Cross-site scripting (XSS) vulnerability in the dismissChangeRelatedObjectPopup function in contrib/admin/static/admin/js/admin/RelatedObjectLookups.js in Django before 1.8.14, 1.9.x before 1.9.8, and 1.10.x before 1.10rc1 allows remote attackers to inject arbitrary web script or HTML via vectors involving unsafe usage of Element.innerHTML.
CVE-2016-6197	fs/overlayfs/dir.c in the OverlayFS filesystem implementation in the Linux kernel before 4.6 does not properly verify the upper dentry before proceeding with unlink and rename system-call processing, which allows local users to cause a denial of service (system crash) via a rename system call that specifies a self-hardlink.
CVE-2016-6207	Integer overflow in the _gdContributionsAlloc function in gd_interpolation.c in GD Graphics Library (aka libgd) before 2.2.3 allows remote attackers to cause a denial of service (out-of-bounds memory write or memory consumption) via unspecified vectors.
CVE-2016-6210	sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.
CVE-2016-6213	fs/namespace.c in the Linux kernel before 4.9 does not restrict how many mounts may exist in a mount namespace, which allows local users to cause a denial of service (memory consumption and deadlock) via MS_BIND mount system calls, as demonstrated by a

	loop that triggers exponential growth in the number of mounts.
CVE-2016-6214	gd_tga.c in the GD Graphics Library (aka libgd) before 2.2.3 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TGA file.
CVE-2016-6223	The TIFFReadRawStrip1 and TIFFReadRawTile1 functions in tif_read.c in libtiff before 4.0.7 allows remote attackers to cause a denial of service (crash) or possibly obtain sensitive information via a negative index in a file-content buffer.
CVE-2016-6224	ecryptfs-setup-swap in eCryptfs does not prevent the unencrypted swap partition from activating during boot when using GPT partitioning on a (1) NVMe or (2) MMC drive, which allows local users to obtain sensitive information via unspecified vectors. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-8946.
CVE-2016-6250	Integer overflow in the ISO9660 writer in libarchive before 3.2.1 allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via vectors related to verifying filename lengths when writing an ISO9660 archive, which trigger a buffer overflow.
CVE-2016-6252	Integer overflow in shadow 4.2.1 allows local users to gain privileges via crafted input to newuidmap.
CVE-2016-6261	The idna_to_ascii_4i function in lib/idna.c in libidn before 1.33 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via 64 bytes of input.
CVE-2016-6262	idn in libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a zero byte as input, which triggers an out-of-bounds read, a different vulnerability than CVE-2015-8948.
CVE-2016-6263	The stringprep_utf8_nfkc_normalize function in lib/nfkc.c in libidn before 1.33 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via crafted UTF-8 data.
CVE-2016-6289	Integer overflow in the virtual_file_ex function in TSRM/tsrm_virtual_cwd.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted extract operation on a ZIP archive.
CVE-2016-6290	ext/session/session.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly maintain a certain hash data structure, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to session deserialization.

CVE-2016-6291	The exif_process_IFD_in_MAKERNOTE function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds array access and memory corruption), obtain sensitive information from process memory, or possibly have unspecified other impact via a crafted JPEG image.
CVE-2016-6292	The exif_process_user_comment function in ext/exif/exif.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted JPEG image.
CVE-2016-6293	The uloc_acceptLanguageFromHTTP function in common/uloc.cpp in International Components for Unicode (ICU) through 57.1 for C/C++ does not ensure that there is a '\0' character at the end of a certain temporary array, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long httpAcceptLanguage argument.
CVE-2016-6294	The locale_accept_from_http function in ext/intl/locale/locale_methods.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly restrict calls to the ICU uloc_acceptLanguageFromHTTP function, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long argument.
CVE-2016-6295	ext/snmp/snmp.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via crafted serialized data, a related issue to CVE-2016-5773.
CVE-2016-6296	Integer signedness error in the simplestring_addn function in simplestring.c in xmlrpc-epi through 0.54.2, as used in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a long first argument to the PHP xmlrpc_encode_request function.
CVE-2016-6297	Integer overflow in the php_stream_zip_opener function in ext/zip/zip_stream.c in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted zip:// URL.
CVE-2016-6302	The tls_decrypt_ticket function in ssl/t1_lib.c in OpenSSL before 1.1.0 does not consider the HMAC

	size during validation of the ticket length, which allows remote attackers to cause a denial of service via a ticket that is too short.
CVE-2016-6303	Integer overflow in the MDC2_Update function in crypto/mdc2/mdc2dgst.c in OpenSSL before 1.1.0 allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2016-6304	Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.
CVE-2016-6306	The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.
CVE-2016-6313	The mixing functions in the random number generator in Libgcrypt before 1.5.6, 1.6.x before 1.6.6, and 1.7.x before 1.7.3 and GnuPG before 1.4.21 make it easier for attackers to obtain the values of 160 bits by leveraging knowledge of the previous 4640 bits.
CVE-2016-6321	Directory traversal vulnerability in the safer_name_suffix function in GNU tar 1.14 through 1.29 might allow remote attackers to bypass an intended protection mechanism and write to arbitrary files via vectors related to improper sanitization of the file_name parameter, aka POINTYFEATHER.
CVE-2016-6323	The makecontext function in the GNU C Library (aka glibc or libc6) before 2.25 creates execution contexts incompatible with the unwinder on ARM EABI (32-bit) platforms, which might allow context-dependent attackers to cause a denial of service (hang), as demonstrated by applications compiled using gccgo, related to backtrace generation.
CVE-2016-6329	OpenVPN, when using a 64-bit block cipher, makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTP-over-OpenVPN session using Blowfish in CBC mode, aka a "Sweet32" attack.
CVE-2016-6351	The esp_do_dma function in hw/scsi/esp.c in QEMU (aka Quick Emulator), when built with ESP/NCR53C9x controller emulation support, allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) or execute arbitrary code on the QEMU host via vectors involving DMA read into ESP command buffer.

CVE-2016-6352	The OneLine32 function in io-ico.c in gdk-pixbuf before 2.35.3 allows remote attackers to cause a denial of service (out-of-bounds write and crash) via crafted dimensions in an ICO file.
CVE-2016-6480	Race condition in the ioctl_send_fib function in drivers/scsi/aacraid/commctrl.c in the Linux kernel through 4.7 allows local users to cause a denial of service (out-of-bounds access or system crash) by changing a certain size value, aka a "double fetch" vulnerability.
CVE-2016-6489	The RSA and DSA decryption code in Nettle makes it easier for attackers to discover private keys via a cache side channel attack.
CVE-2016-6515	The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.
CVE-2016-6662	Oracle MySQL through 5.5.52, 5.6.x through 5.6.33, and 5.7.x through 5.7.15; MariaDB before 5.5.51, 10.0.x before 10.0.27, and 10.1.x before 10.1.17; and Percona Server before 5.5.51-38.1, 5.6.x before 5.6.32-78.0, and 5.7.x before 5.7.14-7 allow local users to create arbitrary configurations and bypass certain protection mechanisms by setting general_log_file to a my.cnf configuration. NOTE: this can be leveraged to execute arbitrary code with root privileges by setting malloc_lib. NOTE: the affected MySQL version information is from Oracle's October 2016 CPU. Oracle has not commented on third-party claims that the issue was silently patched in MySQL 5.5.52, 5.6.33, and 5.7.15.
CVE-2016-6794	When a SecurityManager is configured, a web application's ability to read system properties should be controlled by the SecurityManager. In Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70, 6.0.0 to 6.0.45 the system property replacement feature for configuration files could be used by a malicious web application to bypass the SecurityManager and read system properties that should not be visible.
CVE-2016-6796	A malicious web application running on Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 was able to bypass a configured SecurityManager via manipulation of the configuration parameters for the JSP Servlet.
CVE-2016-6797	The ResourceLinkFactory implementation in Apache Tomcat 9.0.0.M1 to 9.0.0.M9, 8.5.0 to 8.5.4, 8.0.0.RC1 to 8.0.36, 7.0.0 to 7.0.70 and 6.0.0 to 6.0.45 did not limit web application access to global JNDI resources to those resources explicitly linked to the web application. Therefore, it was possible for a web application to

	access any global JNDI resource whether an explicit ResourceLink had been configured or not.
CVE-2016-6816	The code in Apache Tomcat 9.0.0.M1 to 9.0.0.M11, 8.5.0 to 8.5.6, 8.0.0.RC1 to 8.0.38, 7.0.0 to 7.0.72, and 6.0.0 to 6.0.47 that parsed the HTTP request line permitted invalid characters. This could be exploited, in conjunction with a proxy that also permitted the invalid characters but with a different interpretation, to inject data into the HTTP response. By manipulating the HTTP response the attacker could poison a web-cache, perform an XSS attack and/or obtain sensitive information from requests other then their own.
CVE-2016-6828	The tcp_check_send_head function in include/net/tcp.h in the Linux kernel before 4.7.5 does not properly maintain certain SACK state after a failed data copy, which allows local users to cause a denial of service (tcp_xmit_retransmit_queue use-after-free and system crash) via a crafted SACK option.
CVE-2016-6833	Use-after-free vulnerability in the vmxnet3_io_bar0_write function in hw/net/vmxnet3.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (QEMU instance crash) by leveraging failure to check if the device is active.
CVE-2016-6834	The net_tx_pkt_do_sw_fragmentation function in hw/net/net_tx_pkt.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via a zero length for the current fragment length.
CVE-2016-6835	The vmxnet_tx_pkt_parse_headers function in hw/net/vmxnet_tx_pkt.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (buffer over-read) by leveraging failure to check IP header length.
CVE-2016-6836	The vmxnet3_complete_packet function in hw/net/vmxnet3.c in QEMU (aka Quick Emulator) allows local guest OS administrators to obtain sensitive host memory information by leveraging failure to initialize the txcq_descr object.
CVE-2016-6855	Eye of GNOME (aka eog) 3.16.5, 3.17.x, 3.18.x before 3.18.3, 3.19.x, and 3.20.x before 3.20.4, when used with glib before 2.44.1, allow remote attackers to cause a denial of service (out-of-bounds write and crash) via vectors involving passing invalid UTF-8 to GMarkup.
CVE-2016-6888	Integer overflow in the net_tx_pkt_init function in hw/net/net_tx_pkt.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (QEMU process crash) via the maximum fragmentation count, which triggers an unchecked multiplication and NULL pointer dereference.

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-2016-6906	The read_image_tga function in gd_tga.c in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TGA file, related to the decompression buffer.
CVE-2016-6911	The dynamicGetbuf function in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted TIFF image.
CVE-2016-6912	Double free vulnerability in the gdImageWebPtr function in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to have unspecified impact via large width and height values.
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-2016-7035	An authorization flaw was found in Pacemaker before 1.1.16, where it did not properly guard its IPC

	interface. An attacker with an unprivileged account on a Pacemaker node could use this flaw to, for example, force the Local Resource Manager daemon to execute a script as root and thereby gain root access on the machine.
CVE-2016-7039	The IP stack in the Linux kernel through 4.8.2 allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for large crafted packets, as demonstrated by packets that contain only VLAN headers, a related issue to CVE-2016-8666.
CVE-2016-7042	The proc_keys_show function in security/keys/proc.c in the Linux kernel through 4.8.2, when the GNU Compiler Collection (gcc) stack protector is enabled, uses an incorrect buffer size for certain timeout data, which allows local users to cause a denial of service (stack memory corruption and panic) by reading the /proc/keys file.
CVE-2016-7044	The unformat_24bit_color function in the format parsing code in Irssi before 0.8.20, when compiled with true-color enabled, allows remote attackers to cause a denial of service (heap corruption and crash) via an incomplete 24bit color code.
CVE-2016-7045	The format_send_to_gui function in the format parsing code in Irssi before 0.8.20 allows remote attackers to cause a denial of service (heap corruption and crash) via vectors involving the length of a string.
CVE-2016-7055	There is a carry propagating bug in the Broadwell-specific Montgomery multiplication procedure in OpenSSL 1.0.2 and 1.1.0 before 1.1.0c that handles input lengths divisible by, but longer than 256 bits. Analysis suggests that attacks against RSA, DSA and DH private keys are impossible. This is because the subroutine in question is not used in operations with the private key itself and an input of the attacker's direct choice. Otherwise the bug can manifest itself as transient authentication and key negotiation failures or reproducible erroneous outcome of public-key operations with specially crafted input. Among EC algorithms only Brainpool P-512 curves are affected and one presumably can attack ECDH key negotiation. Impact was not analyzed in detail, because pre-requisites for attack are considered unlikely. Namely multiple clients have to choose the curve in question and the server has to share the private key among them, neither of which is default behaviour. Even then only clients that chose the curve will be affected.
CVE-2016-7056	A timing attack flaw was found in OpenSSL 1.0.1u and before that could allow a malicious user with local access to recover ECDSA P-256 private keys.

CVE-2016-7097	The filesystem implementation in the Linux kernel through 4.8.2 preserves the setgid bit during a setxattr call, which allows local users to gain group privileges by leveraging the existence of a setgid program with restrictions on execute permissions.
CVE-2016-7098	Race condition in wget 1.17 and earlier, when used in recursive or mirroring mode to download a single file, might allow remote servers to bypass intended access list restrictions by keeping an HTTP connection open.
CVE-2016-7116	Directory traversal vulnerability in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to access host files outside the export path via a .. (dot dot) in an unspecified string.
CVE-2016-7124	ext/standard/var_unserializer.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles certain invalid objects, which allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted serialized data that leads to a (1) __destruct call or (2) magic method call.
CVE-2016-7125	ext/session/session.c in PHP before 5.6.25 and 7.x before 7.0.10 skips invalid session names in a way that triggers incorrect parsing, which allows remote attackers to inject arbitrary-type session data by leveraging control of a session name, as demonstrated by object injection.
CVE-2016-7127	The imagegammacorrect function in ext/gd/gd.c in PHP before 5.6.25 and 7.x before 7.0.10 does not properly validate gamma values, which allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by providing different signs for the second and third arguments.
CVE-2016-7128	The exif_process_IFD_in_TIFF function in ext/exif/exif.c in PHP before 5.6.25 and 7.x before 7.0.10 mishandles the case of a thumbnail offset that exceeds the file size, which allows remote attackers to obtain sensitive information from process memory via a crafted TIFF image.
CVE-2016-7129	The php_wddx_process_data function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via an invalid ISO 8601 time value, as demonstrated by a wddx_deserialize call that mishandles a dateTime element in a wddxPacket XML document.
CVE-2016-7130	The php_wddx_pop_element function in ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an

	invalid base64 binary value, as demonstrated by a wddx_deserialize call that mishandles a binary element in a wddxPacket XML document.
CVE-2016-7131	ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via a malformed wddxPacket XML document that is mishandled in a wddx_deserialize call, as demonstrated by a tag that lacks a < (less than) character.
CVE-2016-7132	ext/wddx/wddx.c in PHP before 5.6.25 and 7.x before 7.0.10 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or possibly have unspecified other impact via an invalid wddxPacket XML document that is mishandled in a wddx_deserialize call, as demonstrated by a stray element inside a boolean element, leading to incorrect pop processing.
CVE-2016-7133	Zend/zend_alloc.c in PHP 7.x before 7.0.10, when open_basedir is enabled, mishandles huge realloc operations, which allows remote attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact via a long pathname.
CVE-2016-7134	ext/curl/interface.c in PHP 7.x before 7.0.10 does not work around a libcurl integer overflow, which allows remote attackers to cause a denial of service (allocation error and heap-based buffer overflow) or possibly have unspecified other impact via a long string that is mishandled in a curl_escape call.
CVE-2016-7141	curl and libcurl before 7.50.2, when built with NSS and the libnsspem.so library is available at runtime, allow remote attackers to hijack the authentication of a TLS connection by leveraging reuse of a previously loaded client certificate from file for a connection for which no certificate has been set, a different vulnerability than CVE-2016-5420.
CVE-2016-7146	MoinMoin 1.9.8 allows remote attackers to conduct "JavaScript injection" attacks by using the "page creation or crafted URL" approach, related to a "Cross Site Scripting (XSS)" issue affecting the action=fckdialog&dialog=attachment (via page name) component.
CVE-2016-7148	MoinMoin 1.9.8 allows remote attackers to conduct "JavaScript injection" attacks by using the "page creation" approach, related to a "Cross Site Scripting (XSS)" issue affecting the action=AttachFile (via page name) component.
CVE-2016-7155	hw/scsi/vmw_pvscsi.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (out-of-bounds access or infinite loop, and

	QEMU process crash) via a crafted page count for descriptor rings.
CVE-2016-7156	The pvscsi_convert_sglist function in hw/scsi/vmw_pvscsi.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) by leveraging an incorrect cast.
CVE-2016-7161	Heap-based buffer overflow in the .receive callback of xlnx.xps-ethernetlite in QEMU (aka Quick Emulator) allows attackers to execute arbitrary code on the QEMU host via a large ethlite packet.
CVE-2016-7162	The _g_file_remove_directory function in file-utils.c in File Roller 3.5.4 through 3.20.2 allows remote attackers to delete arbitrary files via a symlink attack on a folder in an archive.
CVE-2016-7166	libarchive before 3.2.0 does not limit the number of recursive decompressions, which allows remote attackers to cause a denial of service (memory consumption and application crash) via a crafted gzip file.
CVE-2016-7167	Multiple integer overflows in the (1) curl_escape, (2) curl_easy_escape, (3) curl_unescape, and (4) curl_easy_unescape functions in libcurl before 7.50.3 allow attackers to have unspecified impact via a string of length 0xffffffff, which triggers a heap-based buffer overflow.
CVE-2016-7170	The vmsvga_fifo_run function in hw/display/vmware_vga.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (out-of-bounds write and QEMU process crash) via vectors related to cursor.mask[] and cursor.image[] array sizes when processing a DEFINE_CURSOR svga command.
CVE-2016-7382	For the NVIDIA Quadro, NVS, GeForce, and Tesla products, NVIDIA GPU Display Driver contains a vulnerability in the kernel mode layer (nvlddmkm.sys for Windows or nvidia.ko for Linux) handler where a missing permissions check may allow users to gain access to arbitrary physical memory, leading to an escalation of privileges.
CVE-2016-7389	For the NVIDIA Quadro, NVS, GeForce, and Tesla products, NVIDIA GPU Display Driver on Linux R304 before 304.132, R340 before 340.98, R367 before 367.55, R361_93 before 361.93.03, and R370 before 370.28 contains a vulnerability in the kernel mode layer (nvidia.ko) handler for mmap() where improper input validation may allow users to gain access to arbitrary physical memory, leading to an escalation of privileges.
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-2016-7401	The cookie parsing code in Django before 1.8.15 and 1.9.x before 1.9.10, when used on a site with Google Analytics, allows remote attackers to bypass an intended CSRF protection mechanism by setting arbitrary cookies.
CVE-2016-7412	ext/mysqlnd/mysqlnd_wireprotocol.c in PHP before 5.6.26 and 7.x before 7.0.11 does not verify that a BIT field has the UNSIGNED_FLAG flag, which allows remote MySQL servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted field metadata.
CVE-2016-7413	Use-after-free vulnerability in the wddx_stack_destroy function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a wddxPacket XML document that lacks an end-tag for a recordset field element, leading to mishandling in a wddx_deserialize call.
CVE-2016-7414	The ZIP signature-verification feature in PHP before 5.6.26 and 7.x before 7.0.11 does not ensure that the uncompressed_filesize field is large enough, which allows remote attackers to cause a denial of service (out-of-bounds memory access) or possibly have unspecified other impact via a crafted PHAR archive, related to ext/phar/util.c and ext/phar/zip.c.
CVE-2016-7415	Stack-based buffer overflow in the Locale class in common/locid.cpp in International Components for Unicode (ICU) through 57.1 for C/C++ allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a long locale string.
CVE-2016-7416	ext/intl/msgformat/msgformat_format.c in PHP before 5.6.26 and 7.x before 7.0.11 does not properly restrict the locale length provided to the Locale class in the ICU library, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a MessageFormatter::formatMessage call with a long first argument.
CVE-2016-7417	ext/spl/spl_array.c in PHP before 5.6.26 and 7.x before 7.0.11 proceeds with SplArray unserialization without validating a return value and data type, which allows remote attackers to cause a denial of service

	or possibly have unspecified other impact via crafted serialized data.
CVE-2016-7418	The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.26 and 7.x before 7.0.11 allows remote attackers to cause a denial of service (invalid pointer access and out-of-bounds read) or possibly have unspecified other impact via an incorrect boolean element in a wddxPacket XML document, leading to mishandling in a wddx_deserialize call.
CVE-2016-7421	The pvscsi_ring_pop_req_descr function in hw/scsi/vmw_pvscsi.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) by leveraging failure to limit process IO loop to the ring size.
CVE-2016-7425	The arcmsr_iop_message_xfer function in drivers/scsi/arcmsr/arcmsr_hba.c in the Linux kernel through 4.8.2 does not restrict a certain length field, which allows local users to gain privileges or cause a denial of service (heap-based buffer overflow) via an ARCMSR_MESSAGE_WRITE_WQBUFFER control code.
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-2016-7427	The broadcast mode replay prevention functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (reject broadcast mode packets) via a crafted broadcast mode packet.
CVE-2016-7428	ntpd in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (reject broadcast mode packets) via the poll interval in a broadcast packet.
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-2016-7434	The read_mru_list function in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (crash) via a crafted mrulist query.

CVE-2016-7440	The C software implementation of AES Encryption and Decryption in wolfSSL (formerly CyaSSL) before 3.9.10 makes it easier for local users to discover AES keys by leveraging cache-bank timing differences.
CVE-2016-7444	The gnutls_ocsp_resp_check_crt function in lib/x509/ocsp.c in GnuTLS before 3.4.15 and 3.5.x before 3.5.4 does not verify the serial length of an OCSP response, which might allow remote attackers to bypass an intended certificate validation mechanism via vectors involving trailing bytes left by gnutls_malloc.
CVE-2016-7466	Memory leak in the usb_xhci_exit function in hw/usb/hcd-xhci.c in QEMU (aka Quick Emulator), when the xhci uses msix, allows local guest OS administrators to cause a denial of service (memory consumption and possibly QEMU process crash) by repeatedly unplugging a USB device.
CVE-2016-7479	In all versions of PHP 7, during the unserialization process, resizing the 'properties' hash table of a serialized object may lead to use-after-free. A remote attacker may exploit this bug to gain arbitrary code execution.
CVE-2016-7543	Bash before 4.4 allows local users to execute arbitrary commands with root privileges via crafted SHELLOPTS and PS4 environment variables.
CVE-2016-7549	Google Chrome before 53.0.2785.113 does not ensure that the recipient of a certain IPC message is a valid RenderFrame or RenderWidget, which allows remote attackers to cause a denial of service (invalid pointer dereference and application crash) or possibly have unspecified other impact by leveraging access to a renderer process, related to render_frame_host_impl.cc and render_widget_host_impl.cc, as demonstrated by a Password Manager message.
CVE-2016-7553	The buf.pl script before 2.20 in Irssi before 0.8.20 uses weak permissions for the scrollbuffer dump file created between upgrades, which might allow local users to obtain sensitive information from private chat conversations by reading the file.
CVE-2016-7568	Integer overflow in the gdImageWebpCtx function in gd_webp.c in the GD Graphics Library (aka libgd) through 2.2.3, as used in PHP through 7.0.11, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via crafted imagewebp and imagedestroy calls.
CVE-2016-7578	An issue was discovered in certain Apple products. iOS before 10.1 is affected. Safari before 10.0.1 is affected. iCloud before 6.0.1 is affected. iTunes before 12.5.2 is affected. tvOS before 10.0.1 is affected. The issue involves the "WebKit" component. It allows remote

	attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2016-7586	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive information via a crafted web site.
CVE-2016-7589	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. watchOS before 3.1.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2016-7592	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component, which allows remote attackers to obtain sensitive information via crafted JavaScript prompts on a web site.
CVE-2016-7599	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site that uses HTTP redirects.
CVE-2016-7623	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive information via a blob URL on a web site.
CVE-2016-7632	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2016-7635	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2016-7639	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2016-7641	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2016-7645	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2016-7652	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2016-7654	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2016-7656	An issue was discovered in certain Apple products. iOS before 10.2 is affected. Safari before 10.0.2 is affected. iCloud before 6.1 is affected. iTunes before 12.5.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2016-7797	Pacemaker before 1.1.15, when using pacemaker remote, might allow remote attackers to cause a denial of service (node disconnection) via an unauthenticated connection.
CVE-2016-7798	The openssl gem for Ruby uses the same initialization vector (IV) in GCM Mode (aes-*-gcm) when the IV is set before the key, which makes it easier for

	context-dependent attackers to bypass the encryption protection mechanism.
CVE-2016-7799	MagickCore/profile.c in ImageMagick before 7.0.3-2 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file.
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-2016-7906	magick/attribute.c in ImageMagick 7.0.3-2 allows remote attackers to cause a denial of service (use-after-free) via a crafted file.
CVE-2016-7907	The imx_fec_do_tx function in hw/net/imx_fec.c in QEMU (aka Quick Emulator) does not properly limit the buffer descriptor count when transmitting packets, which allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via vectors involving a buffer descriptor with a length of 0 and crafted values in bd.flags.
CVE-2016-7908	The mcf_fec_do_tx function in hw/net/mcf_fec.c in QEMU (aka Quick Emulator) does not properly limit the buffer descriptor count when transmitting packets, which allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) via vectors involving a buffer descriptor with a length of 0 and crafted values in bd.flags.
CVE-2016-7909	The pcnet_rdra_addr function in hw/net/pcnet.c in QEMU (aka Quick Emulator) allows local guest OS

	administrators to cause a denial of service (infinite loop and QEMU process crash) by setting the (1) receive or (2) transmit descriptor ring length to 0.
CVE-2016-7913	The xc2028_set_config function in drivers/media/tuners/tuner-xc2028.c in the Linux kernel before 4.6 allows local users to gain privileges or cause a denial of service (use-after-free) via vectors involving omission of the firmware name from a certain data structure.
CVE-2016-7917	The nfnetlink_rcv_batch function in net/netfilter/nfnetlink.c in the Linux kernel before 4.5 does not check whether a batch message's length field is large enough, which allows local users to obtain sensitive information from kernel memory or cause a denial of service (infinite loop or out-of-bounds read) by leveraging the CAP_NET_ADMIN capability.
CVE-2016-7922	The AH parser in tcpdump before 4.9.0 has a buffer overflow in print-ah.c:ah_print().
CVE-2016-7923	The ARP parser in tcpdump before 4.9.0 has a buffer overflow in print-arp.c:arp_print().
CVE-2016-7924	The ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-atm.c:oam_print().
CVE-2016-7925	The compressed SLIP parser in tcpdump before 4.9.0 has a buffer overflow in print-sl.c:sl_if_print().
CVE-2016-7926	The Ethernet parser in tcpdump before 4.9.0 has a buffer overflow in print-ether.c:ethertype_print().
CVE-2016-7927	The IEEE 802.11 parser in tcpdump before 4.9.0 has a buffer overflow in print-802_11.c:ieee802_11_radio_print().
CVE-2016-7928	The IPComp parser in tcpdump before 4.9.0 has a buffer overflow in print-ipcomp.c:ipcomp_print().
CVE-2016-7929	The Juniper PPPoE ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-juniper.c:juniper_parse_header().
CVE-2016-7930	The LLC/SNAP parser in tcpdump before 4.9.0 has a buffer overflow in print-llc.c:llc_print().
CVE-2016-7931	The MPLS parser in tcpdump before 4.9.0 has a buffer overflow in print-mpls.c:mpls_print().
CVE-2016-7932	The PIM parser in tcpdump before 4.9.0 has a buffer overflow in print-pim.c:pimv2_check_checksum().
CVE-2016-7933	The PPP parser in tcpdump before 4.9.0 has a buffer overflow in print-ppp.c:ppp_hdlc_if_print().
CVE-2016-7934	The RTCP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:rtcp_print().
CVE-2016-7935	The RTP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:rtp_print().
CVE-2016-7936	The UDP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:udp_print().

CVE-2016-7937	The VAT parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:vat_print().
CVE-2016-7938	The ZeroMQ parser in tcpdump before 4.9.0 has an integer overflow in print-zeromq.c:zmtp1_print_frame().
CVE-2016-7939	The GRE parser in tcpdump before 4.9.0 has a buffer overflow in print-gre.c, multiple functions.
CVE-2016-7940	The STP parser in tcpdump before 4.9.0 has a buffer overflow in print-stp.c, multiple functions.
CVE-2016-7942	The XGetImage function in X.org libX11 before 1.6.4 might allow remote X servers to gain privileges via vectors involving image type and geometry, which triggers out-of-bounds read operations.
CVE-2016-7943	The XListFonts function in X.org libX11 before 1.6.4 might allow remote X servers to gain privileges via vectors involving length fields, which trigger out-of-bounds write operations.
CVE-2016-7973	The AppleTalk parser in tcpdump before 4.9.0 has a buffer overflow in print-atalk.c, multiple functions.
CVE-2016-7974	The IP parser in tcpdump before 4.9.0 has a buffer overflow in print-ip.c, multiple functions.
CVE-2016-7975	The TCP parser in tcpdump before 4.9.0 has a buffer overflow in print-tcp.c:tcp_print().
CVE-2016-7976	The PS Interpreter in Ghostscript 9.18 and 9.20 allows remote attackers to execute arbitrary code via crafted userparams.
CVE-2016-7977	Ghostscript before 9.21 might allow remote attackers to bypass the SAFER mode protection mechanism and consequently read arbitrary files via the use of the .libfile operator in a crafted postscript document.
CVE-2016-7978	Use-after-free vulnerability in Ghostscript 9.20 might allow remote attackers to execute arbitrary code via vectors related to a reference leak in .setdevice.
CVE-2016-7979	Ghostscript before 9.21 might allow remote attackers to bypass the SAFER mode protection mechanism and consequently execute arbitrary code by leveraging type confusion in .initialize_dsc_parser.
CVE-2016-7983	The BOOTP parser in tcpdump before 4.9.0 has a buffer overflow in print-bootp.c:bootp_print().
CVE-2016-7984	The TFTP parser in tcpdump before 4.9.0 has a buffer overflow in print-tftp.c:tftp_print().
CVE-2016-7985	The CALM FAST parser in tcpdump before 4.9.0 has a buffer overflow in print-calm-fast.c:calm_fast_print().
CVE-2016-7986	The GeoNetworking parser in tcpdump before 4.9.0 has a buffer overflow in print-geonet.c, multiple functions.
CVE-2016-7992	The Classical IP over ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-cip.c:cip_if_print().

CVE-2016-7993	A bug in util-print.c:relts_print() in tcpdump before 4.9.0 could cause a buffer overflow in multiple protocol parsers (DNS, DVMRP, HSRP, IGMP, lightweight resolver protocol, PIM).
CVE-2016-7994	Memory leak in the virtio_gpu_resource_create_2d function in hw/display/virtio-gpu.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption) via a large number of VIRTIO_GPU_CMD_RESOURCE_CREATE_2D commands.
CVE-2016-8318	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.8 (Availability impacts).
CVE-2016-8327	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.4 (Availability impacts).
CVE-2016-8331	An exploitable remote code execution vulnerability exists in the handling of TIFF images in LibTIFF version 4.0.6. A crafted TIFF document can lead to a type confusion vulnerability resulting in remote code execution. This vulnerability can be triggered via a TIFF file delivered to the application using LibTIFF's tag extension functionality.
CVE-2016-8399	An elevation of privilege vulnerability in the kernel networking subsystem could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Moderate because it first requires compromising a privileged process and current compiler optimizations restrict access to the vulnerable code. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31349935.

CVE-2016-8405	An information disclosure vulnerability in kernel components including the ION subsystem, Binder, USB driver and networking subsystem could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31651010.
CVE-2016-8574	The FRF.15 parser in tcpdump before 4.9.0 has a buffer overflow in print-fr.c:frf15_print().
CVE-2016-8575	The Q.933 parser in tcpdump before 4.9.0 has a buffer overflow in print-fr.c:q933_print(), a different vulnerability than CVE-2017-5482.
CVE-2016-8576	The xhci_ring_fetch function in hw/usb/hcd-xhci.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and QEMU process crash) by leveraging failure to limit the number of link Transfer Request Blocks (TRB) to process.
CVE-2016-8577	Memory leak in the v9fs_read function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption) via vectors related to an I/O read operation.
CVE-2016-8578	The v9fs_iov_vunmarshal function in fsdev/9p-iov-marshal.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (NULL pointer dereference and QEMU process crash) by sending an empty string parameter to a 9P operation.
CVE-2016-8602	The .sethalftone5 function in psi/zht2.c in Ghostscript before 9.21 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted Postscript document that calls .sethalftone5 with an empty operand stack.
CVE-2016-8610	A denial of service flaw was found in OpenSSL 0.9.8, 1.0.1, 1.0.2 through 1.0.2h, and 1.1.0 in the way the TLS/SSL protocol defined processing of ALERT packets during a connection handshake. A remote attacker could use this flaw to make a TLS/SSL server consume an excessive amount of CPU and fail to accept connections from other clients.
CVE-2016-8615	A flaw was found in curl before version 7.51. If cookie state is written into a cookie jar file that is later read back and used for subsequent requests, a malicious HTTP server can inject new cookies for arbitrary domains into said cookie jar.
CVE-2016-8616	A flaw was found in curl before version 7.51.0 When re-using a connection, curl was doing case insensitive comparisons of user name and password with the

	existing connections. This means that if an unused connection with proper credentials exists for a protocol that has connection-scoped credentials, an attacker can cause that connection to be reused if s/he knows the case-insensitive version of the correct password.
CVE-2016-8617	The base64 encode function in curl before version 7.51.0 is prone to a buffer being under allocated in 32bit systems if it receives at least 1Gb as input via `CURLOPT_USERNAME`.
CVE-2016-8618	The libcurl API function called `curl_maprintf()` before version 7.51.0 can be tricked into doing a double-free due to an unsafe `size_t` multiplication, on systems using 32 bit `size_t` variables.
CVE-2016-8619	The function `read_data()` in security.c in curl before version 7.51.0 is vulnerable to memory double free.
CVE-2016-8620	The 'globbing' feature in curl before version 7.51.0 has a flaw that leads to integer overflow and out-of-bounds read via user controlled input.
CVE-2016-8621	The `curl_getdate` function in curl before version 7.51.0 is vulnerable to an out of bounds read if it receives an input with one digit short.
CVE-2016-8622	The URL percent-encoding decode function in libcurl before 7.51.0 is called `curl_easy_unescape`. Internally, even if this function would be made to allocate a unscape destination buffer larger than 2GB, it would return that new length in a signed 32 bit integer variable, thus the length would get either just truncated or both truncated and turned negative. That could then lead to libcurl writing outside of its heap based buffer.
CVE-2016-8623	A flaw was found in curl before version 7.51.0. The way curl handles cookies permits other threads to trigger a use-after-free leading to information disclosure.
CVE-2016-8624	curl before version 7.51.0 doesn't parse the authority component of the URL correctly when the host name part ends with a '#' character, and could instead be tricked into connecting to a different host. This may have security implications if you for example use an URL parser that follows the RFC to check for allowed domains before using curl to request them.
CVE-2016-8630	The x86_decode_insn function in arch/x86/kvm/emulate.c in the Linux kernel before 4.8.7, when KVM is enabled, allows local users to cause a denial of service (host OS crash) via a certain use of a ModR/M byte in an undefined instruction.
CVE-2016-8632	The tipc_msg_build function in net/tipc/msg.c in the Linux kernel through 4.8.11 does not validate the relationship between the minimum fragment length and the maximum packet size, which allows local users to gain privileges or cause a denial of service (heap-based

	buffer overflow) by leveraging the CAP_NET_ADMIN capability.
CVE-2016-8633	drivers/firewire/net.c in the Linux kernel before 4.8.7, in certain unusual hardware configurations, allows remote attackers to execute arbitrary code via crafted fragmented packets.
CVE-2016-8635	It was found that Diffie Hellman Client key exchange handling in NSS 3.21.x was vulnerable to small subgroup confinement attack. An attacker could use this flaw to recover private keys by confining the client DH key to small subgroup of the desired group.
CVE-2016-8636	Integer overflow in the mem_check_range function in drivers/infiniband/sw/rxe/rxe_mr.c in the Linux kernel before 4.9.10 allows local users to cause a denial of service (memory corruption), obtain sensitive information from kernel memory, or possibly have unspecified other impact via a write or read request involving the "RDMA protocol over infiniband" (aka Soft RoCE) technology.
CVE-2016-8645	The TCP stack in the Linux kernel before 4.8.10 mishandles skb truncation, which allows local users to cause a denial of service (system crash) via a crafted application that makes sendto system calls, related to net/ipv4/tcp_ipv4.c and net/ipv6/tcp_ipv6.c.
CVE-2016-8649	lxc-attach in LXC before 1.0.9 and 2.x before 2.0.6 allows an attacker inside of an unprivileged container to use an inherited file descriptor, of the host's /proc, to access the rest of the host's filesystem via the openat() family of syscalls.
CVE-2016-8654	A heap-buffer overflow vulnerability was found in QMFB code in JPC codec caused by buffer being allocated with too small size. jasper versions before 2.0.0 are affected.
CVE-2016-8655	Race condition in net/packet/af_packet.c in the Linux kernel through 4.8.12 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging the CAP_NET_RAW capability to change a socket version, related to the packet_set_ring and packet_setsockopt functions.
CVE-2016-8658	Stack-based buffer overflow in the brcmf_cfg80211_start_ap function in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c in the Linux kernel before 4.7.5 allows local users to cause a denial of service (system crash) or possibly have unspecified other impact via a long SSID Information Element in a command to a Netlink socket.
CVE-2016-8667	The rc4030_write function in hw/dma/rc4030.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (divide-by-

	zero error and QEMU process crash) via a large interval timer reload value.
CVE-2016-8668	The rocker_io_writel function in hw/net/rocker/rocker.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (out-of-bounds read and QEMU process crash) by leveraging failure to limit DMA buffer size.
CVE-2016-8669	The serial_update_parameters function in hw/char/serial.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (divide-by-zero error and QEMU process crash) via vectors involving a value of divider greater than baud base.
CVE-2016-8670	Integer signedness error in the dynamicGetbuf function in gd_io_dp.c in the GD Graphics Library (aka libgd) through 2.2.3, as used in PHP before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a crafted imagecreatefromstring call.
CVE-2016-8677	The AcquireQuantumPixels function in MagickCore/quantum.c in ImageMagick before 7.0.3-1 allows remote attackers to have unspecified impact via a crafted image file, which triggers a memory allocation failure.
CVE-2016-8687	Stack-based buffer overflow in the safe_fprintf function in tar/util.c in libarchive 3.2.1 allows remote attackers to cause a denial of service via a crafted non-printable multibyte character in a filename.
CVE-2016-8688	The mtree bidder in libarchive 3.2.1 does not keep track of line sizes when extending the read-ahead, which allows remote attackers to cause a denial of service (crash) via a crafted file, which triggers an invalid read in the (1) detect_form or (2) bid_entry function in libarchive/archive_read_support_format_mtree.c.
CVE-2016-8689	The read_Header function in archive_read_support_format_7zip.c in libarchive 3.2.1 allows remote attackers to cause a denial of service (out-of-bounds read) via multiple EmptyStream attributes in a header in a 7zip archive.
CVE-2016-8691	The jpc_dec_process_siz function in libjasper/jpc/jpc_dec.c in JasPer before 1.900.4 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted XRsiz value in a BMP image to the imginfo command.
CVE-2016-8692	The jpc_dec_process_siz function in libjasper/jpc/jpc_dec.c in JasPer before 1.900.4 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted YRsiz value in a BMP image to the imginfo command.

CVE-2016-8693	Double free vulnerability in the mem_close function in jas_stream.c in JasPer before 1.900.10 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted BMP image to the imginfo command.
CVE-2016-8704	An integer overflow in the process_bin_append_prepend function in Memcached, which is responsible for processing multiple commands of Memcached binary protocol, can be abused to cause heap overflow and lead to remote code execution.
CVE-2016-8705	Multiple integer overflows in process_bin_update function in Memcached, which is responsible for processing multiple commands of Memcached binary protocol, can be abused to cause heap overflow and lead to remote code execution.
CVE-2016-8706	An integer overflow in process_bin_sasl_auth function in Memcached, which is responsible for authentication commands of Memcached binary protocol, can be abused to cause heap overflow and lead to remote code execution.
CVE-2016-8707	An exploitable out of bounds write exists in the handling of compressed TIFF images in ImageMagicks's convert utility. A crafted TIFF document can lead to an out of bounds write which in particular circumstances could be leveraged into remote code execution. The vulnerability can be triggered through any user controlled TIFF that is handled by this functionality.
CVE-2016-8734	Subversion's mod_dontdothat module and HTTP clients 1.4.0 through 1.8.16, and 1.9.0 through 1.9.4 are vulnerable to a denial-of-service attack caused by exponential XML entity expansion. The attack can cause the targeted process to consume an excessive amount of CPU resources or memory.
CVE-2016-8735	Remote code execution is possible with Apache Tomcat before 6.0.48, 7.x before 7.0.73, 8.x before 8.0.39, 8.5.x before 8.5.7, and 9.x before 9.0.0.M12 if JmxRemoteLifecycleListener is used and an attacker can reach JMX ports. The issue exists because this listener wasn't updated for consistency with the CVE-2016-3427 Oracle patch that affected credential types.
CVE-2016-8743	Apache HTTP Server, in all releases prior to 2.2.32 and 2.4.25, was liberal in the whitespace accepted from requests and sent in response lines and headers. Accepting these different behaviors represented a security concern when httpd participates in any chain of proxies or interacts with back-end application servers, either through mod_proxy or using conventional CGI mechanisms, and may result in request smuggling, response splitting and cache pollution.

CVE-2016-8745	A bug in the error handling of the send file code for the NIO HTTP connector in Apache Tomcat 9.0.0.M1 to 9.0.0.M13, 8.5.0 to 8.5.8, 8.0.0.RC1 to 8.0.39, 7.0.0 to 7.0.73 and 6.0.16 to 6.0.48 resulted in the current Processor object being added to the Processor cache multiple times. This in turn meant that the same Processor could be used for concurrent requests. Sharing a Processor can result in information leakage between requests including, not not limited to, session ID and the response body. The bug was first noticed in 8.5.x onwards where it appears the refactoring of the Connector code for 8.5.x onwards made it more likely that the bug was observed. Initially it was thought that the 8.5.x refactoring introduced the bug but further investigation has shown that the bug is present in all currently supported Tomcat versions.
CVE-2016-8826	All versions of NVIDIA GPU Display Driver contain a vulnerability in the kernel mode layer (nvlddmkm.sys for Windows or nvidia.ko for Linux) where a user can cause a GPU interrupt storm, leading to a denial of service.
CVE-2016-8862	The AcquireMagickMemory function in MagickCore/memory.c in ImageMagick before 7.0.3.3 allows remote attackers to have unspecified impact via a crafted image, which triggers a memory allocation failure.
CVE-2016-8864	named in ISC BIND 9.x before 9.9.9-P4, 9.10.x before 9.10.4-P4, and 9.11.x before 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a DNAME record in the answer section of a response to a recursive query, related to db.c and resolver.c.
CVE-2016-8882	The jpc_dec_tilefini function in libjasper/jpc/jpc_dec.c in JasPer before 1.900.8 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted file.
CVE-2016-8883	The jpc_dec_tiledecode function in jpc_dec.c in JasPer before 1.900.8 allows remote attackers to cause a denial of service (assertion failure) via a crafted file.
CVE-2016-8887	The jp2_colr_destroy function in libjasper/jp2/jp2_cod.c in JasPer before 1.900.10 allows remote attackers to cause a denial of service (NULL pointer dereference).
CVE-2016-8909	The intel_hda_xfer function in hw/audio/intel-hda.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and CPU consumption) via an entry with the same value for buffer length and pointer position.
CVE-2016-8910	The rtl8139_cplus_transmit function in hw/net/rtl8139.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (infinite loop and CPU consumption) by leveraging failure to limit the ring descriptor count.

CVE-2016-9013	Django 1.8.x before 1.8.16, 1.9.x before 1.9.11, and 1.10.x before 1.10.3 use a hardcoded password for a temporary database user created when running tests with an Oracle database, which makes it easier for remote attackers to obtain access to the database server by leveraging failure to manually specify a password in the database settings TEST dictionary.
CVE-2016-9014	Django before 1.8.x before 1.8.16, 1.9.x before 1.9.11, and 1.10.x before 1.10.3, when settings.DEBUG is True, allow remote attackers to conduct DNS rebinding attacks by leveraging failure to validate the HTTP Host header against settings.ALLOWED_HOSTS.
CVE-2016-9063	An integer overflow during the parsing of XML using the Expat library. This vulnerability affects Firefox < 50.
CVE-2016-9064	Add-on updates failed to verify that the add-on ID inside the signed package matched the ID of the add-on being updated. An attacker who could perform a man-in-the-middle attack on the user's connection to the update server and defeat the certificate pinning protection could provide a malicious signed add-on instead of a valid update. This vulnerability affects Firefox ESR < 45.5 and Firefox < 50.
CVE-2016-9066	A buffer overflow resulting in a potentially exploitable crash due to memory allocation issues when handling large amounts of incoming data. This vulnerability affects Thunderbird < 45.5, Firefox ESR < 45.5, and Firefox < 50.
CVE-2016-9067	Two use-after-free errors during DOM operations resulting in potentially exploitable crashes. This vulnerability affects Firefox < 50.
CVE-2016-9068	A use-after-free during web animations when working with timelines resulting in a potentially exploitable crash. This vulnerability affects Firefox < 50.
CVE-2016-9069	A use-after-free in nsINode::ReplaceOrInsertBefore during DOM operations resulting in potentially exploitable crashes. This vulnerability affects Firefox < 50.
CVE-2016-9070	A maliciously crafted page loaded to the sidebar through a bookmark can reference a privileged chrome window and engage in limited JavaScript operations violating cross-origin protections. This vulnerability affects Firefox < 50.
CVE-2016-9071	Content Security Policy combined with HTTP to HTTPS redirection can be used by malicious server to verify whether a known site is within a user's browser history. This vulnerability affects Firefox < 50.
CVE-2016-9073	WebExtensions can bypass security checks to load privileged URLs and potentially escape the

	WebExtension sandbox. This vulnerability affects Firefox < 50.
CVE-2016-9074	An existing mitigation of timing side-channel attacks is insufficient in some circumstances. This issue is addressed in Network Security Services (NSS) 3.26.1. This vulnerability affects Thunderbird < 45.5, Firefox ESR < 45.5, and Firefox < 50.
CVE-2016-9075	An issue where WebExtensions can use the mozAddonManager API to elevate privilege due to privileged pages being allowed in the permissions list. This allows a malicious extension to then install additional extensions without explicit user permission. This vulnerability affects Firefox < 50.
CVE-2016-9076	An issue where a "<select>" dropdown menu can be used to cover location bar content, resulting in potential spoofing attacks. This attack requires e10s to be enabled in order to function. This vulnerability affects Firefox < 50.
CVE-2016-9077	Canvas allows the use of the "feDisplacementMap" filter on images loaded cross-origin. The rendering by the filter is variable depending on the input pixel, allowing for timing attacks when the images are loaded from third party locations. This vulnerability affects Firefox < 50.
CVE-2016-9078	Redirection from an HTTP connection to a "data:" URL assigns the referring site's origin to the "data:" URL in some circumstances. This can result in same-origin violations against a domain if it loads resources from malicious sites. Cross-origin setting of cookies has been demonstrated without the ability to read them. Note: This issue only affects Firefox 49 and 50. This vulnerability affects Firefox < 50.0.1.
CVE-2016-9079	A use-after-free vulnerability in SVG Animation has been discovered. An exploit built on this vulnerability has been discovered in the wild targeting Firefox and Tor Browser users on Windows. This vulnerability affects Firefox < 50.0.2, Firefox ESR < 45.5.1, and Thunderbird < 45.5.1.
CVE-2016-9080	Memory safety bugs were reported in Firefox 50.0.2. 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 < 50.1.
CVE-2016-9083	drivers/vfio/pci/vfio_pci.c in the Linux kernel through 4.8.11 allows local users to bypass integer overflow checks, and cause a denial of service (memory corruption) or have unspecified other impact, by leveraging access to a vfio PCI device file for a VFIO_DEVICE_SET_IRQS ioctl call, aka a "state machine confusion bug."

CVE-2016-9084	drivers/vfio/pci/vfio_pci_intrs.c in the Linux kernel through 4.8.11 misuses the kzalloc function, which allows local users to cause a denial of service (integer overflow) or have unspecified other impact by leveraging access to a vfio PCI device file.
CVE-2016-9101	Memory leak in hw/net/eepro100.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption and QEMU process crash) by repeatedly unplugging an i8255x (PRO100) NIC device.
CVE-2016-9102	Memory leak in the v9fs_xattrcreate function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption and QEMU process crash) via a large number of Txattrcreate messages with the same fid number.
CVE-2016-9103	The v9fs_xattrcreate function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to obtain sensitive host heap memory information by reading xattribute values before writing to them.
CVE-2016-9104	Multiple integer overflows in the (1) v9fs_xattr_read and (2) v9fs_xattr_write functions in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allow local guest OS administrators to cause a denial of service (QEMU process crash) via a crafted offset, which triggers an out-of-bounds access.
CVE-2016-9105	Memory leak in the v9fs_link function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption) via vectors involving a reference to the source fid object.
CVE-2016-9106	Memory leak in the v9fs_write function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS administrators to cause a denial of service (memory consumption) by leveraging failure to free an IO vector.
CVE-2016-9119	Cross-site scripting (XSS) vulnerability in the link dialogue in GUI editor in MoinMoin before 1.9.8 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2016-9131	named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed response to an RTYPE ANY query.
CVE-2016-9137	Use-after-free vulnerability in the CURLFile implementation in ext/curl/curl_file.c in PHP before 5.6.27 and 7.x before 7.0.12 allows remote attackers to cause a denial of service or possibly have unspecified

	other impact via crafted serialized data that is mishandled during __wakeup processing.
CVE-2016-9147	named in ISC BIND 9.9.9-P4, 9.9.9-S6, 9.10.4-P4, and 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a response containing an inconsistency among the DNSSEC-related RRsets.
CVE-2016-9178	The __get_user_asm_ex macro in arch/x86/include/asm/uaccess.h in the Linux kernel before 4.7.5 does not initialize a certain integer variable, which allows local users to obtain sensitive information from kernel stack memory by triggering failure of a get_user_ex call.
CVE-2016-9189	Pillow before 3.3.2 allows context-dependent attackers to obtain sensitive information by using the "crafted image file" approach, related to an "Integer Overflow" issue affecting the Image.core.map_buffer in map.c component.
CVE-2016-9190	Pillow before 3.3.2 allows context-dependent attackers to execute arbitrary code by using the "crafted image file" approach, related to an "Insecure Sign Extension" issue affecting the ImagingNew in Storage.c component.
CVE-2016-9191	The cgroup offline implementation in the Linux kernel through 4.8.11 mishandles certain drain operations, which allows local users to cause a denial of service (system hang) by leveraging access to a container environment for executing a crafted application, as demonstrated by trinity.
CVE-2016-9243	HKDF in cryptography before 1.5.2 returns an empty byte-string if used with a length less than algorithm.digest_size.
CVE-2016-9262	Multiple integer overflows in the (1) jas_realloc function in base/jas_malloc.c and (2) mem_resize function in base/jas_stream.c in JasPer before 1.900.22 allow remote attackers to cause a denial of service via a crafted image, which triggers use after free vulnerabilities.
CVE-2016-9273	tiffsplit in libtiff 4.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted file, related to changing td_nstrips in TIFF_STRIPCHOP mode.
CVE-2016-9297	The TIFFFetchNormalTag function in LibTiff 4.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) via crafted TIFF_SETGET_C16ASCII or TIFF_SETGET_C32_ASCII tag values.
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-2016-9317	The gdImageCreate function in the GD Graphics Library (aka libgd) before 2.2.4 allows remote attackers to cause a denial of service (system hang) via an oversized image.
CVE-2016-9318	libxml2 2.9.4 and earlier, as used in XMLSec 1.2.23 and earlier and other products, does not offer a flag directly indicating that the current document may be read but other files may not be opened, which makes it easier for remote attackers to conduct XML External Entity (XXE) attacks via a crafted document.
CVE-2016-9381	Race condition in QEMU in Xen allows local x86 HVM guest OS administrators to gain privileges by changing certain data on shared rings, aka a "double fetch" vulnerability.
CVE-2016-9387	Integer overflow in the jpc_dec_process_siz function in libjasper/jpc/jpc_dec.c in JasPer before 1.900.13 allows remote attackers to have unspecified impact via a crafted file, which triggers an assertion failure.
CVE-2016-9388	The ras_getcmap function in ras_dec.c in JasPer before 1.900.14 allows remote attackers to cause a denial of service (assertion failure) via a crafted image file.
CVE-2016-9389	The jpc_irct and jpc_iict functions in jpc_mct.c in JasPer before 1.900.14 allow remote attackers to cause a denial of service (assertion failure).
CVE-2016-9390	The jas_seq2d_create function in jas_seq.c in JasPer before 1.900.14 allows remote attackers to cause a denial of service (assertion failure) via a crafted image file.
CVE-2016-9391	The jpc_bitstream_getbits function in jpc_bs.c in JasPer before 2.0.10 allows remote attackers to cause a denial of service (assertion failure) via a very large integer.
CVE-2016-9392	The calcstepsizes function in jpc_dec.c in JasPer before 1.900.17 allows remote attackers to cause a denial of service (assertion failure) via a crafted file.
CVE-2016-9393	The jpc_pi_nextrpcl function in jpc_t2cod.c in JasPer before 1.900.17 allows remote attackers to cause a denial of service (assertion failure) via a crafted file.
CVE-2016-9394	The jas_seq2d_create function in jas_seq.c in JasPer before 1.900.17 allows remote attackers to cause a denial of service (assertion failure) via a crafted file.
CVE-2016-9396	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-2016-9401	popd in bash might allow local users to bypass the restricted shell and cause a use-after-free via a crafted address.
CVE-2016-9427	Integer overflow vulnerability in bdwgc before 2016-09-27 allows attackers to cause client of bdwgc denial of service (heap buffer overflow crash) and possibly execute arbitrary code via huge allocation.
CVE-2016-9444	named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted DS resource record in an answer.
CVE-2016-9448	The TIFFFetchNormalTag function in LibTiff 4.0.6 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) by setting the tags TIFF_SETGET_C16ASCII or TIFF_SETGET_C32_ASCII to values that access 0-byte arrays. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-9297.
CVE-2016-9453	The t2p_readwrite_pdf_image_tile function in LibTIFF allows remote attackers to cause a denial of service (out-of-bounds write and crash) or possibly execute arbitrary code via a JPEG file with a TIFFTAG_JPEGTABLES of length one.
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-2016-9533	tif_pixarlog.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in heap allocated buffers. Reported as MSVR 35094, aka "PixarLog horizontalDifference heap-buffer-overflow."
CVE-2016-9534	tif_write.c in libtiff 4.0.6 has an issue in the error code path of TIFFFlushData1() that didn't reset the tif_rawcc and tif_rawcp members. Reported as MSVR 35095, aka "TIFFFlushData1 heap-buffer-overflow."
CVE-2016-9535	tif_predict.h and tif_predict.c in libtiff 4.0.6 have assertions that can lead to assertion failures in debug mode, or buffer overflows in release mode, when dealing with unusual tile size like YCbCr with subsampling. Reported as MSVR 35105, aka "Predictor heap-buffer-overflow."
CVE-2016-9536	tools/tiff2pdf.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in heap allocated buffers in t2p_process_jpeg_strip(). Reported as MSVR 35098, aka "t2p_process_jpeg_strip heap-buffer-overflow."
CVE-2016-9537	tools/tiffcrop.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in buffers. Reported as MSVR 35093, MSVR 35096, and MSVR 35097.

CVE-2016-9538	tools/tiffcrop.c in libtiff 4.0.6 reads an undefined buffer in readContigStripsIntoBuffer() because of a uint16 integer overflow. Reported as MSVR 35100.
CVE-2016-9539	tools/tiffcrop.c in libtiff 4.0.6 has an out-of-bounds read in readContigTilesIntoBuffer(). Reported as MSVR 35092.
CVE-2016-9540	tools/tiffcp.c in libtiff 4.0.6 has an out-of-bounds write on tiled images with odd tile width versus image width. Reported as MSVR 35103, aka "cpStripToTile heap-buffer-overflow."
CVE-2016-9555	The sctp_sf_ootb function in net/sctp/sm_statefuns.c in the Linux kernel before 4.8.8 lacks chunk-length checking for the first chunk, which allows remote attackers to cause a denial of service (out-of-bounds slab access) or possibly have unspecified other impact via crafted SCTP data.
CVE-2016-9556	The IsPixelGray function in MagickCore/pixel-accessor.h in ImageMagick 7.0.3-8 allows remote attackers to cause a denial of service (out-of-bounds heap read) via a crafted image file.
CVE-2016-9560	Stack-based buffer overflow in the jpc_tsfb_getbands2 function in jpc_tsfb.c in JasPer before 1.900.30 allows remote attackers to have unspecified impact via a crafted image.
CVE-2016-9566	base/logging.c in Nagios Core before 4.2.4 allows local users with access to an account in the nagios group to gain root privileges via a symlink attack on the log file. NOTE: this can be leveraged by remote attackers using CVE-2016-9565.
CVE-2016-9577	A vulnerability was discovered in SPICE before 0.13.90 in the server's protocol handling. An authenticated attacker could send crafted messages to the SPICE server causing a heap overflow leading to a crash or possible code execution.
CVE-2016-9578	A vulnerability was discovered in SPICE before 0.13.90 in the server's protocol handling. An attacker able to connect to the SPICE server could send crafted messages which would cause the process to crash.
CVE-2016-9586	curl before version 7.52.0 is vulnerable to a buffer overflow when doing a large floating point output in libcurl's implementation of the printf() functions. If there are any application that accepts a format string from the outside without necessary input filtering, it could allow remote attacks.
CVE-2016-9588	arch/x86/kvm/vmx.c in the Linux kernel through 4.9 mismanages the #BP and #OF exceptions, which allows guest OS users to cause a denial of service (guest OS crash) by declining to handle an exception thrown by an L2 guest.

CVE-2016-9591	JasPer before version 2.0.12 is vulnerable to a use-after-free in the way it decodes certain JPEG 2000 image files resulting in a crash on the application using JasPer.
CVE-2016-9600	JasPer before version 2.0.10 is vulnerable to a null pointer dereference was found in the decoded creation of JPEG 2000 image files. A specially crafted file could cause an application using JasPer to crash.
CVE-2016-9601	ghostscript before version 9.21 is vulnerable to a heap based buffer overflow that was found in the ghostscript jbig2_decode_gray_scale_image function which is used to decode halftone segments in a JBIG2 image. A document (PostScript or PDF) with an embedded, specially crafted, jbig2 image could trigger a segmentation fault in ghostscript.
CVE-2016-9602	Qemu before version 2.9 is vulnerable to an improper link following when built with the VirtFS. A privileged user inside guest could use this flaw to access host file system beyond the shared folder and potentially escalating their privileges on a host.
CVE-2016-9603	A heap buffer overflow flaw was found in QEMU's Cirrus CLGD 54xx VGA emulator's VNC display driver support before 2.9; the issue could occur when a VNC client attempted to update its display after a VGA operation is performed by a guest. A privileged user/process inside a guest could use this flaw to crash the QEMU process or, potentially, execute arbitrary code on the host with privileges of the QEMU process.
CVE-2016-9604	It was discovered in the Linux kernel before 4.11-rc8 that root can gain direct access to an internal keyring, such as '.dns_resolver' in RHEL-7 or '.builtin_trusted_keys' upstream, by joining it as its session keyring. This allows root to bypass module signature verification by adding a new public key of its own devising to the keyring.
CVE-2016-9642	JavaScriptCore in WebKit allows attackers to cause a denial of service (out-of-bounds heap read) via a crafted Javascript file.
CVE-2016-9643	The regex code in Webkit 2.4.11 allows remote attackers to cause a denial of service (memory consumption) as demonstrated in a large number of ($ (open parenthesis and dollar) followed by {-2,16} and a large number of +) (plus close parenthesis).
CVE-2016-9644	The __get_user_asm_ex macro in arch/x86/include/asm/uaccess.h in the Linux kernel 4.4.22 through 4.4.28 contains extended asm statements that are incompatible with the exception table, which allows local users to obtain root access on non-SMEP platforms via a crafted application. NOTE: this

	vulnerability exists because of incorrect backporting of the CVE-2016-9178 patch to older kernels.
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	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2016-9755	The netfilter subsystem in the Linux kernel before 4.9 mishandles IPv6 reassembly, which allows local users to cause a denial of service (integer overflow, out-of-bounds write, and GPF) or possibly have unspecified other impact via a crafted application that makes socket, connect, and writev system calls, related to net/ipv6/netfilter/nf_conntrack_reasm.c and net/ipv6/netfilter/nf_defrag_ipv6_hooks.c.
CVE-2016-9756	arch/x86/kvm/emulate.c in the Linux kernel before 4.8.12 does not properly initialize Code Segment (CS) in certain error cases, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.
CVE-2016-9774	The postinst script in the tomcat6 package before 6.0.45+dfsg-1~deb7u4 on Debian wheezy, before 6.0.35-1ubuntu3.9 on Ubuntu 12.04 LTS and on Ubuntu 14.04 LTS; the tomcat7 package before 7.0.28-4+deb7u8 on Debian wheezy, before 7.0.56-3+deb8u6 on Debian jessie, before 7.0.52-1ubuntu0.8 on Ubuntu 14.04 LTS, and on Ubuntu 12.04 LTS, 16.04 LTS, and 16.10; and the tomcat8 package before 8.0.14-1+deb8u5 on Debian jessie, before 8.0.32-1ubuntu1.3 on Ubuntu 16.04 LTS, before 8.0.37-1ubuntu0.1 on Ubuntu 16.10, and before 8.0.38-2ubuntu1 on Ubuntu 17.04 might allow local users with access to the tomcat account to obtain sensitive information or gain root privileges via a symlink attack on the Catalina localhost directory.
CVE-2016-9775	The postrm script in the tomcat6 package before 6.0.45+dfsg-1~deb7u3 on Debian wheezy, before 6.0.45+dfsg-1~deb8u1 on Debian jessie, before 6.0.35-1ubuntu3.9 on Ubuntu 12.04 LTS and on Ubuntu 14.04 LTS; the tomcat7 package before 7.0.28-4+deb7u7 on Debian wheezy, before 7.0.56-3+deb8u6 on Debian jessie, before

	7.0.52-1ubuntu0.8 on Ubuntu 14.04 LTS, and on Ubuntu 12.04 LTS, 16.04 LTS, and 16.10; and the tomcat8 package before 8.0.14-1+deb8u5 on Debian jessie, before 8.0.32-1ubuntu1.3 on Ubuntu 16.04 LTS, before 8.0.37-1ubuntu0.1 on Ubuntu 16.10, and before 8.0.38-2ubuntu1 on Ubuntu 17.04 might allow local users with access to the tomcat account to gain root privileges via a setgid program in the Catalina directory, as demonstrated by /etc/tomcat8/Catalina/attack.
CVE-2016-9776	QEMU (aka Quick Emulator) built with the ColdFire Fast Ethernet Controller emulator support is vulnerable to an infinite loop issue. It could occur while receiving packets in 'mcf_fec_receive'. A privileged user/process inside guest could use this issue to crash the QEMU process on the host leading to DoS.
CVE-2016-9793	The sock_setsockopt function in net/core/sock.c in the Linux kernel before 4.8.14 mishandles negative values of sk_sndbuf and sk_rcvbuf, which allows local users to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact by leveraging the CAP_NET_ADMIN capability for a crafted setsockopt system call with the (1) SO_SNDBUFFORCE or (2) SO_RCVBUFFORCE option.
CVE-2016-9794	Race condition in the snd_pcm_period_elapsed function in sound/core/pcm_lib.c in the ALSA subsystem in the Linux kernel before 4.7 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted SNDRV_PCM_TRIGGER_START command.
CVE-2016-9811	The windows_icon_typefind function in gst-plugins-base in GStreamer before 1.10.2, when G_SLICE is set to always-malloc, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted ico file.
CVE-2016-9845	QEMU (aka Quick Emulator) built with the Virtio GPU Device emulator support is vulnerable to an information leakage issue. It could occur while processing 'VIRTIO_GPU_CMD_GET_CAPSET_INFO' command. A guest user/process could use this flaw to leak contents of the host memory bytes.
CVE-2016-9846	QEMU (aka Quick Emulator) built with the Virtio GPU Device emulator support is vulnerable to a memory leakage issue. It could occur while updating the cursor data in update_cursor_data_virgl. A guest user/process could use this flaw to leak host memory bytes, resulting in DoS for a host.
CVE-2016-9877	An issue was discovered in Pivotal RabbitMQ 3.x before 3.5.8 and 3.6.x before 3.6.6 and RabbitMQ for PCF 1.5.x before 1.5.20, 1.6.x before 1.6.12, and 1.7.x before 1.7.7. MQTT (MQ Telemetry Transport)

	connection authentication with a username/password pair succeeds if an existing username is provided but the password is omitted from the connection request. Connections that use TLS with a client-provided certificate are not affected.
CVE-2016-9893	Memory safety bugs were reported in Thunderbird 45.5. 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 Firefox < 50.1, Firefox ESR < 45.6, and Thunderbird < 45.6.
CVE-2016-9894	A buffer overflow in SkiaGl caused when a GrGLBuffer is truncated during allocation. Later writers will overflow the buffer, resulting in a potentially exploitable crash. This vulnerability affects Firefox < 50.1.
CVE-2016-9895	Event handlers on "marquee" elements were executed despite a strict Content Security Policy (CSP) that disallowed inline JavaScript. This vulnerability affects Firefox < 50.1, Firefox ESR < 45.6, and Thunderbird < 45.6.
CVE-2016-9896	Use-after-free while manipulating the "navigator" object within WebVR. Note: WebVR is not currently enabled by default. This vulnerability affects Firefox < 50.1.
CVE-2016-9897	Memory corruption resulting in a potentially exploitable crash during WebGL functions using a vector constructor with a varying array within libGLES. This vulnerability affects Firefox < 50.1, Firefox ESR < 45.6, and Thunderbird < 45.6.
CVE-2016-9898	Use-after-free resulting in potentially exploitable crash when manipulating DOM subtrees in the Editor. This vulnerability affects Firefox < 50.1, Firefox ESR < 45.6, and Thunderbird < 45.6.
CVE-2016-9899	Use-after-free while manipulating DOM events and removing audio elements due to errors in the handling of node adoption. This vulnerability affects Firefox < 50.1, Firefox ESR < 45.6, and Thunderbird < 45.6.
CVE-2016-9900	External resources that should be blocked when loaded by SVG images can bypass security restrictions through the use of "data:" URLs. This could allow for cross-domain data leakage. This vulnerability affects Firefox < 50.1, Firefox ESR < 45.6, and Thunderbird < 45.6.
CVE-2016-9901	HTML tags received from the Pocket server will be processed without sanitization and any JavaScript code executed will be run in the "about:pocket-saved" (unprivileged) page, giving it access to Pocket's messaging API through HTML injection. This vulnerability affects Firefox ESR < 45.6 and Firefox < 50.1.

CVE-2016-9902	The Pocket toolbar button, once activated, listens for events fired from it's own pages but does not verify the origin of incoming events. This allows content from other origins to fire events and inject content and commands into the Pocket context. Note: this issue does not affect users with e10s enabled. This vulnerability affects Firefox ESR < 45.6 and Firefox < 50.1.
CVE-2016-9903	Mozilla's add-ons SDK had a world-accessible resource with an HTML injection vulnerability. If an additional vulnerability allowed this resource to be loaded as a document it could allow injecting content and script into an add-on's context. This vulnerability affects Firefox < 50.1.
CVE-2016-9904	An attacker could use a JavaScript Map/Set timing attack to determine whether an atom is used by another compartment/zone in specific contexts. This could be used to leak information, such as usernames embedded in JavaScript code, across websites. This vulnerability affects Firefox < 50.1, Firefox ESR < 45.6, and Thunderbird < 45.6.
CVE-2016-9905	A potentially exploitable crash in "EnumerateSubDocuments" while adding or removing sub-documents. This vulnerability affects Firefox ESR < 45.6 and Thunderbird < 45.6.
CVE-2016-9907	Quick Emulator (Qemu) built with the USB redirector usb-guest support is vulnerable to a memory leakage flaw. It could occur while destroying the USB redirector in 'usbredir_handle_destroy'. A guest user/process could use this issue to leak host memory, resulting in DoS for a host.
CVE-2016-9908	Quick Emulator (Qemu) built with the Virtio GPU Device emulator support is vulnerable to an information leakage issue. It could occur while processing 'VIRTIO_GPU_CMD_GET_CAPSET' command. A guest user/process could use this flaw to leak contents of the host memory bytes.
CVE-2016-9909	The serializer in html5lib before 0.99999999 might allow remote attackers to conduct cross-site scripting (XSS) attacks by leveraging mishandling of the < (less than) character in attribute values.
CVE-2016-9910	The serializer in html5lib before 0.99999999 might allow remote attackers to conduct cross-site scripting (XSS) attacks by leveraging mishandling of special characters in attribute values, a different vulnerability than CVE-2016-9909.
CVE-2016-9911	Quick Emulator (Qemu) built with the USB EHCI Emulation support is vulnerable to a memory leakage issue. It could occur while processing packet data in

	'ehci_init_transfer'. A guest user/process could use this issue to leak host memory, resulting in DoS for a host.
CVE-2016-9912	Quick Emulator (Qemu) built with the Virtio GPU Device emulator support is vulnerable to a memory leakage issue. It could occur while destroying gpu resource object in 'virtio_gpu_resource_destroy'. A guest user/process could use this flaw to leak host memory bytes, resulting in DoS for a host.
CVE-2016-9913	Memory leak in the v9fs_device_unrealize_common function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local privileged guest OS users to cause a denial of service (host memory consumption and possibly QEMU process crash) via vectors involving the order of resource cleanup.
CVE-2016-9914	Memory leak in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local privileged guest OS users to cause a denial of service (host memory consumption and possibly QEMU process crash) by leveraging a missing cleanup operation in FileOperations.
CVE-2016-9915	Memory leak in hw/9pfs/9p-handle.c in QEMU (aka Quick Emulator) allows local privileged guest OS users to cause a denial of service (host memory consumption and possibly QEMU process crash) by leveraging a missing cleanup operation in the handle backend.
CVE-2016-9916	Memory leak in hw/9pfs/9p-proxy.c in QEMU (aka Quick Emulator) allows local privileged guest OS users to cause a denial of service (host memory consumption and possibly QEMU process crash) by leveraging a missing cleanup operation in the proxy backend.
CVE-2016-9921	Quick emulator (Qemu) built with the Cirrus CLGD 54xx VGA Emulator support is vulnerable to a divide by zero issue. It could occur while copying VGA data when cirrus graphics mode was set to be VGA. A privileged user inside guest could use this flaw to crash the Qemu process instance on the host, resulting in DoS.
CVE-2016-9922	The cirrus_do_copy function in hw/display/cirrus_vga.c in QEMU (aka Quick Emulator), when cirrus graphics mode is VGA, allows local guest OS privileged users to cause a denial of service (divide-by-zero error and QEMU process crash) via vectors involving blit pitch values.
CVE-2016-9933	Stack consumption vulnerability in the gdImageFillToBorder function in gd.c in the GD Graphics Library (aka libgd) before 2.2.2, as used in PHP before 5.6.28 and 7.x before 7.0.13, allows remote attackers to cause a denial of service (segmentation violation) via a crafted imagefilltoborder call that triggers use of a negative color value.
CVE-2016-9935	The php_wddx_push_element function in ext/wddx/wddx.c in PHP before 5.6.29 and 7.x before 7.0.14

	allows remote attackers to cause a denial of service (out-of-bounds read and memory corruption) or possibly have unspecified other impact via an empty boolean element in a wddxPacket XML document.
CVE-2016-9936	The unserialize implementation in ext/standard/var.c in PHP 7.x before 7.0.14 allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted serialized data. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-6834.
CVE-2016-9941	Heap-based buffer overflow in rfbproto.c in LibVNCClient in LibVNCServer before 0.9.11 allows remote servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted FramebufferUpdate message containing a subrectangle outside of the client drawing area.
CVE-2016-9942	Heap-based buffer overflow in ultra.c in LibVNCClient in LibVNCServer before 0.9.11 allows remote servers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted FramebufferUpdate message with the Ultra type tile, such that the LZO payload decompressed length exceeds what is specified by the tile dimensions.
CVE-2016-9949	An issue was discovered in Apport before 2.20.4. In apport/ui.py, Apport reads the CrashDB field and it then evaluates the field as Python code if it begins with a "{". This allows remote attackers to execute arbitrary Python code.
CVE-2016-9950	An issue was discovered in Apport before 2.20.4. There is a path traversal issue in the Apport crash file "Package" and "SourcePackage" fields. These fields are used to build a path to the package specific hook files in the /usr/share/apport/package-hooks/ directory. An attacker can exploit this path traversal to execute arbitrary Python files from the local system.
CVE-2016-9951	An issue was discovered in Apport before 2.20.4. A malicious Apport crash file can contain a restart command in `RespawnCommand` or `ProcCmdline` fields. This command will be executed if a user clicks the Relaunch button on the Apport prompt from the malicious crash file. The fix is to only show the Relaunch button on Apport crash files generated by local systems. The Relaunch button will be hidden when crash files are opened directly in Apport-GTK.
CVE-2016-9962	RunC allowed additional container processes via 'runc exec' to be ptraced by the pid 1 of the container. This allows the main processes of the container, if running as root, to gain access to file-descriptors of these new processes during the initialization and can lead to

	container escapes or modification of runC state before the process is fully placed inside the container.
CVE-2016-9963	Exim before 4.87.1 might allow remote attackers to obtain the private DKIM signing key via vectors related to log files and bounce messages.
CVE-2017-0318	All versions of NVIDIA Linux GPU Display Driver contain a vulnerability in the kernel mode layer handler where improper validation of an input parameter may cause a denial of service on the system.
CVE-2017-0350	All versions of the NVIDIA GPU Display Driver contain a vulnerability in the kernel mode layer handler where a value passed from a user to the driver is not correctly validated and used in an offset calculation may lead to denial of service or potential escalation of privileges.
CVE-2017-0351	All versions of the NVIDIA GPU Display Driver contain a vulnerability in the kernel mode layer handler where a NULL pointer dereference caused by invalid user input may lead to denial of service or potential escalation of privileges.
CVE-2017-0352	All versions of the NVIDIA GPU Display Driver contain a vulnerability in the GPU firmware where incorrect access control may allow CPU access sensitive GPU control registers, leading to an escalation of privileges
CVE-2017-0357	A heap-overflow flaw exists in the -tr loader of iucode-tool starting with v1.4 and before v2.1.1, potentially leading to SIGSEGV, or heap corruption.
CVE-2017-0358	Jann Horn of Google Project Zero discovered that NTFS-3G, a read-write NTFS driver for FUSE, does not scrub the environment before executing modprobe with elevated privileges. A local user can take advantage of this flaw for local root privilege escalation.
CVE-2017-0553	An elevation of privilege vulnerability in libnl could enable a local malicious application to execute arbitrary code within the context of the Wi-Fi service. This issue is rated as Moderate because it first requires compromising a privileged process and is mitigated by current platform configurations. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32342065. NOTE: this issue also exists in the upstream libnl before 3.3.0 library.
CVE-2017-0663	A remote code execution vulnerability in libxml2 could enable an attacker using a specially crafted file to execute arbitrary code within the context of an unprivileged process. This issue is rated as High due to the possibility of remote code execution in an application that uses this library. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37104170.

CVE-2017-0861	Use-after-free vulnerability in the snd_pcm_info function in the ALSA subsystem in the Linux kernel allows attackers to gain privileges via unspecified vectors.
CVE-2017-0898	Ruby before 2.4.2, 2.3.5, and 2.2.8 is vulnerable to a malicious format string which contains a precious specifier (*) with a huge minus value. Such situation can lead to a buffer overrun, resulting in a heap memory corruption or an information disclosure from the heap.
CVE-2017-0901	RubyGems version 2.6.12 and earlier fails to validate specification names, allowing a maliciously crafted gem to potentially overwrite any file on the filesystem.
CVE-2017-0902	RubyGems version 2.6.12 and earlier is vulnerable to a DNS hijacking vulnerability that allows a MITM attacker to force the RubyGems client to download and install gems from a server that the attacker controls.
CVE-2017-0903	RubyGems versions between 2.0.0 and 2.6.13 are vulnerable to a possible remote code execution vulnerability. YAML deserialization of gem specifications can bypass class white lists. Specially crafted serialized objects can possibly be used to escalate to remote code execution.
CVE-2017-1000024	Shotwell version 0.24.4 or earlier and 0.25.3 or earlier is vulnerable to an information disclosure in the web publishing plugins resulting in potential password and oauth token plaintext transmission
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-2017-1000083	backend/comics/comics-document.c (aka the comic book backend) in GNOME Evince before 3.24.1 allows remote attackers to execute arbitrary commands via a .cbt file that is a TAR archive containing a filename beginning with a "--" command-line option substring, as demonstrated by a --checkpoint-action=exec=bash at the beginning of the filename.
CVE-2017-1000100	When doing a TFTP transfer and curl/libcurl is given a URL that contains a very long file name (longer than about 515 bytes), the file name is truncated to fit within the buffer boundaries, but the buffer size is still wrongly updated to use the untruncated length. This too large value is then used in the sendto() call, making curl attempt to send more data than what is actually put into the buffer. The endto() function will then read beyond the end of the heap based buffer. A malicious HTTP(S) server could redirect a vulnerable libcurl-using client to a crafted TFTP URL (if the client hasn't restricted which protocols it allows redirects to) and trick it to send private memory contents to a remote server over UDP.

	Limit curl's redirect protocols with --proto-redir and libcurl's with CURLOPT_REDIR_PROTOCOLS.
CVE-2017-1000101	curl supports "globbing" of URLs, in which a user can pass a numerical range to have the tool iterate over those numbers to do a sequence of transfers. In the globbing function that parses the numerical range, there was an omission that made curl read a byte beyond the end of the URL if given a carefully crafted, or just wrongly written, URL. The URL is stored in a heap based buffer, so it could then be made to wrongly read something else instead of crashing. An example of a URL that triggers the flaw would be `http://ur %20[0-60000000000000000000`.
CVE-2017-1000111	Linux kernel: heap out-of-bounds in AF_PACKET sockets. This new issue is analogous to previously disclosed CVE-2016-8655. In both cases, a socket option that changes socket state may race with safety checks in packet_set_ring. Previously with PACKET_VERSION. This time with PACKET_RESERVE. The solution is similar: lock the socket for the update. This issue may be exploitable, we did not investigate further. As this issue affects PF_PACKET sockets, it requires CAP_NET_RAW in the process namespace. But note that with user namespaces enabled, any process can create a namespace in which it has CAP_NET_RAW.
CVE-2017-1000112	Linux kernel: Exploitable memory corruption due to UFO to non-UFO path switch. When building a UFO packet with MSG_MORE __ip_append_data() calls ip_ufo_append_data() to append. However in between two send() calls, the append path can be switched from UFO to non-UFO one, which leads to a memory corruption. In case UFO packet lengths exceeds MTU, copy = maxfraglen - skb->len becomes negative on the non-UFO path and the branch to allocate new skb is taken. This triggers fragmentation and computation of fraggap = skb_prev->len - maxfraglen. Fraggap can exceed MTU, causing copy = datalen - transhdrlen - fraggap to become negative. Subsequently skb_copy_and_csum_bits() writes out-of-bounds. A similar issue is present in IPv6 code. The bug was introduced in e89e9cf539a2 ("[IPv4/IPv6]: UFO Scatter-gather approach") on Oct 18 2005.
CVE-2017-1000117	A malicious third-party can give a crafted "ssh://..." URL to an unsuspecting victim, and an attempt to visit the URL can result in any program that exists on the victim's machine being executed. Such a URL could be placed in the .gitmodules file of a malicious project, and an unsuspecting victim could be tricked into running "git clone --recurse-submodules" to trigger the vulnerability.

CVE-2017-1000158	CPython (aka Python) up to 2.7.13 is vulnerable to an integer overflow in the PyString_DecodeEscape function in stringobject.c, resulting in heap-based buffer overflow (and possible arbitrary code execution)
CVE-2017-1000159	Command injection in evince via filename when printing to PDF. This affects versions earlier than 3.25.91.
CVE-2017-1000229	Integer overflow bug in function minitiff_read_info() of optipng 0.7.6 allows an attacker to remotely execute code or cause denial of service.
CVE-2017-1000231	A double-free vulnerability in parse.c in ldns 1.7.0 have unspecified impact and attack vectors.
CVE-2017-1000232	A double-free vulnerability in str2host.c in ldns 1.7.0 have unspecified impact and attack vectors.
CVE-2017-1000242	Jenkins Git Client Plugin 2.4.2 and earlier creates temporary file with insecure permissions resulting in information disclosure
CVE-2017-1000250	All versions of the SDP server in BlueZ 5.46 and earlier are vulnerable to an information disclosure vulnerability which allows remote attackers to obtain sensitive information from the bluetoothd process memory. This vulnerability lies in the processing of SDP search attribute requests.
CVE-2017-1000251	The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 2.6.32 and up to and including 4.13.1, are vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in Remote code execution in kernel space.
CVE-2017-1000252	The KVM subsystem in the Linux kernel through 4.13.3 allows guest OS users to cause a denial of service (assertion failure, and hypervisor hang or crash) via an out-of bounds guest_irq value, related to arch/x86/kvm/vmx.c and virt/kvm/eventfd.c.
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-2017-1000255	On Linux running on PowerPC hardware (Power8 or later) a user process can craft a signal frame and then do a sigreturn so that the kernel will take an exception (interrupt), and use the r1 value *from the signal frame* as the kernel stack pointer. As part of the exception entry the content of the signal frame is written to the kernel stack, allowing an attacker to overwrite arbitrary locations with arbitrary values. The exception handling does produce an oops, and a panic if panic_on_oops=1, but only after kernel memory has been over written. This flaw was introduced in commit: "5d176f751ee3 (powerpc: tm: Enable transactional memory (TM) lazily for userspace)" which was merged upstream into v4.9-rc1. Please note that kernels built with CONFIG_PPC_TRANSACTIONAL_MEM=n are not vulnerable.
CVE-2017-1000256	libvirt version 2.3.0 and later is vulnerable to a bad default configuration of "verify-peer=no" passed to QEMU by libvirt resulting in a failure to validate SSL/TLS certificates by default.
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-2017-1000363	Linux drivers/char/lp.c Out-of-Bounds Write. Due to a missing bounds check, and the fact that parport_ptr integer is static, a 'secure boot' kernel command line adversary (can happen due to bootloader vulns, e.g. Google Nexus 6's CVE-2016-10277, where due to a vulnerability the adversary has partial control over the command line) can overflow the parport_nr array in the following code, by appending many (>LP_NO) 'lp=none' arguments to the command line.

CVE-2017-1000364	An issue was discovered in the size of the stack guard page on Linux, specifically a 4k stack guard page is not sufficiently large and can be "jumped" over (the stack guard page is bypassed), this affects Linux Kernel versions 4.11.5 and earlier (the stackguard page was introduced in 2010).
CVE-2017-1000365	The Linux Kernel imposes a size restriction on the arguments and environmental strings passed through RLIMIT_STACK/RLIM_INFINITY (1/4 of the size), but does not take the argument and environment pointers into account, which allows attackers to bypass this limitation. This affects Linux Kernel versions 4.11.5 and earlier. It appears that this feature was introduced in the Linux Kernel version 2.6.23.
CVE-2017-1000366	glibc contains a vulnerability that allows specially crafted LD_LIBRARY_PATH values to manipulate the heap/stack, causing them to alias, potentially resulting in arbitrary code execution. Please note that additional hardening changes have been made to glibc to prevent manipulation of stack and heap memory but these issues are not directly exploitable, as such they have not been given a CVE. This affects glibc 2.25 and earlier.
CVE-2017-1000367	Todd Miller's sudo version 1.8.20 and earlier is vulnerable to an input validation (embedded spaces) in the get_process_ttyname() function resulting in information disclosure and command execution.
CVE-2017-1000369	Exim supports the use of multiple "-p" command line arguments which are malloc()'ed and never free()'ed, used in conjunction with other issues allows attackers to cause arbitrary code execution. This affects exim version 4.89 and earlier. Please note that at this time upstream has released a patch (commit 65e061b76867a9ea7aeeb535341b790b90ae6c21), but it is not known if a new point release is available that addresses this issue at this time.
CVE-2017-1000380	sound/core/timer.c in the Linux kernel before 4.11.5 is vulnerable to a data race in the ALSA /dev/snd/timer driver resulting in local users being able to read information belonging to other users, i.e., uninitialized memory contents may be disclosed when a read and an ioctl happen at the same time.
CVE-2017-1000381	The c-ares function `ares_parse_naptr_reply()`, which is used for parsing NAPTR responses, could be triggered to read memory outside of the given input buffer if the passed in DNS response packet was crafted in a particular way.
CVE-2017-1000385	The Erlang otp TLS server answers with different TLS alerts to different error types in the RSA PKCS #1 1.5 padding. This allows an attacker to decrypt content or

	sign messages with the server's private key (this is a variation of the Bleichenbacher attack).
CVE-2017-1000405	The Linux Kernel versions 2.6.38 through 4.14 have a problematic use of pmd_mkdirty() in the touch_pmd() 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.
CVE-2017-1000407	The Linux Kernel 2.6.32 and later are affected by a denial of service, by flooding the diagnostic port 0x80 an exception can be triggered leading to a kernel panic.
CVE-2017-1000408	A memory leak in glibc 2.1.1 (released on May 24, 1999) can be reached and amplified through the LD_HWCAP_MASK environment variable. Please note that many versions of glibc are not vulnerable to this issue if patched for CVE-2017-1000366.
CVE-2017-1000409	A buffer overflow in glibc 2.5 (released on September 29, 2006) and can be triggered through the LD_LIBRARY_PATH environment variable. Please note that many versions of glibc are not vulnerable to this issue if patched for CVE-2017-1000366.
CVE-2017-1000422	Gnome gdk-pixbuf 2.36.8 and older is vulnerable to several integer overflow in the gif_get_lzw function resulting in memory corruption and potential code execution
CVE-2017-1000433	pysaml2 version 4.4.0 and older accept any password when run with python optimizations enabled. This allows attackers to log in as any user without knowing their password.
CVE-2017-1000445	ImageMagick 7.0.7-1 and older version are vulnerable to null pointer dereference in the MagickCore component and might lead to denial of service
CVE-2017-1000456	freedesktop.org libpoppler 0.60.1 fails to validate boundaries in TextPool::addWord, leading to overflow in subsequent calculations.
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-2017-1000494	Uninitialized stack variable vulnerability in NameValueParserEndElt (upnpreplyparse.c) in miniupnpd < 2.0 allows an attacker to cause Denial of Service (Segmentation fault and Memory Corruption) or possibly have unspecified other impact
CVE-2017-1000501	Awstats version 7.6 and earlier is vulnerable to a path traversal flaw in the handling of the "config" and "migrate" parameters resulting in unauthenticated remote code execution.
CVE-2017-10053	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2017-10067	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).
CVE-2017-10074	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected

	are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10078	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Scripting). The supported version that is affected is Java SE: 8u131. Easily exploitable vulnerability allows low privileged 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 as well as unauthorized access to critical data or complete access to all Java SE accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 8.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N).
CVE-2017-10081	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments,

	typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2017-10087	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10089	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: ImageIO). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6

	(Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10090	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u141 and 8u131; Java SE Embedded: 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10096	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).

CVE-2017-10101	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10102	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. While the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS 3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).
CVE-2017-10107	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly

	impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10108	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2017-10109	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0

	Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2017-10110	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: AWT). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10111	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). The supported version that is affected is Java SE: 8u131; Java SE Embedded: 8u131. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10115	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JCE). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded:

	8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2017-10116	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10118	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JCE). Supported versions that are affected are Java SE: 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the

	specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2017-10135	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JCE). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2017-10140	Postfix before 2.11.10, 3.0.x before 3.0.10, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 might allow local users to gain privileges by leveraging undocumented functionality in Berkeley DB 2.x and later, related to reading settings from DB_CONFIG in the current directory.
CVE-2017-10155	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Pluggable Auth). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 and earlier. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-10165	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.19 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-2017-10167	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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-2017-10176	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2017-10193	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1

	(Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).
CVE-2017-10195	Vulnerability in the Oracle Hospitality Simphony component of Oracle Hospitality Applications (subcomponent: Import/Export). The supported version that is affected is 2.8. Easily exploitable vulnerability allows unauthenticated attacker with network access via HTTP to compromise Oracle Hospitality Simphony. 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 Hospitality Simphony accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2017-10196	Vulnerability in the Oracle Outside In Technology component of Oracle Fusion Middleware (subcomponent: Outside In Filters). The supported version that is affected is 8.5.3.0. 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 ability to cause a hang or frequently repeatable crash (complete DOS) of Oracle Outside In Technology as well as unauthorized update, insert or delete access to some of Oracle Outside In Technology accessible data. CVSS 3.0 Base Score 8.2 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H).
CVE-2017-10197	Vulnerability in the Oracle Hospitality OPERA 5 Property Services component of Oracle Hospitality Applications (subcomponent: Folios). The supported version that is affected is 5.4.2.x through 5.5.1.x. Easily exploitable vulnerability allows physical access to compromise Oracle Hospitality OPERA 5 Property Services. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Oracle Hospitality OPERA 5 Property Services accessible data. CVSS 3.0 Base Score 4.6 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2017-10198	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional

	products. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 6.8 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N).
CVE-2017-10227	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 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-2017-10243	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JAX-WS). Supported versions that are affected are Java SE: 6u151, 7u141 and 8u131; Java SE Embedded: 8u131; JRockit: R28.3.14. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded, JRockit accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 6.5 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L).
CVE-2017-10268	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-2017-10274	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Smart Card IO). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9. 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 creation, deletion or modification access to critical data or all Java SE accessible data as well as 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, 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 and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N).
CVE-2017-10276	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: FTS). Supported versions that are affected are 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 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-2017-10281	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit.

	Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2017-10283	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 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 ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-10285	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10286	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently

	repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-10294	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 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-2017-10295	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. Difficult to exploit vulnerability allows unauthenticated attacker with network access via HTTP to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 4.0 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:L/A:N).
CVE-2017-10311	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: FTS). Supported versions that are affected are 5.7.19 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-2017-10313	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Group Replication GCS). Supported versions that are affected are 5.7.19 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-2017-10314	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.37 and earlier and 5.7.19 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-2017-10320	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.19 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-2017-10345	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. 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 ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 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-2017-10346	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-10347	Vulnerability in the Java SE, JRockit component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2017-10348	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. 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, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2017-10349	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. 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, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2017-10350	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: JAX-WS). Supported versions that are affected are Java SE: 7u151, 8u144 and 9; Java SE Embedded: 8u144. 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, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).

CVE-2017-10355	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2017-10356	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144; JRockit: R28.3.15. Easily exploitable vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, Java SE Embedded, JRockit executes to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 6.2 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2017-10357	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Serialization). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. 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, that load and

	run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2017-10378	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-2017-10388	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u161, 7u151, 8u144 and 9; Java SE Embedded: 8u144. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Kerberos 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 takeover of Java SE, Java SE Embedded. Note: Applies to the Java SE Kerberos client. CVSS 3.0 Base Score 7.5 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H).
CVE-2017-10663	The sanity_check_ckpt function in fs/f2fs/super.c in the Linux kernel before 4.12.4 does not validate the blkoff and segno arrays, which allows local users to gain privileges via unspecified vectors.
CVE-2017-10664	qemu-nbd in QEMU (aka Quick Emulator) does not ignore SIGPIPE, which allows remote attackers to cause a denial of service (daemon crash) by disconnecting during a server-to-client reply attempt.
CVE-2017-10672	Use-after-free in the XML-LibXML module through 2.0129 for Perl allows remote attackers to execute arbitrary code by controlling the arguments to a replaceChild call.
CVE-2017-10688	In LibTIFF 4.0.8, there is a assertion abort in the TIFFWriteDirectoryTagCheckedLong8Array function in tif_dirwrite.c. A crafted input will lead to a remote denial of service attack.
CVE-2017-10708	An issue was discovered in Apport through 2.20.x. In apport/report.py, Apport sets the ExecutablePath field and it then uses the path to run package specific hooks without protecting against path traversal. This allows remote attackers to execute arbitrary code via a crafted .crash file.
CVE-2017-10784	The Basic authentication code in WEBrick library in Ruby before 2.2.8, 2.3.x before 2.3.5, and 2.4.x through 2.4.1 allows remote attackers to inject terminal emulator escape sequences into its log and possibly execute arbitrary commands via a crafted user name.
CVE-2017-10790	The _asn1_check_identifier function in GNU Libtasn1 through 4.12 causes a NULL pointer dereference and crash when reading crafted input that triggers assignment of a NULL value within an asn1_node structure. It may lead to a remote denial of service attack.
CVE-2017-10806	Stack-based buffer overflow in hw/usb/redirect.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (QEMU process crash) via vectors related to logging debug messages.
CVE-2017-10810	Memory leak in the virtio_gpu_object_create function in drivers/gpu/drm/virtio/virtgpu_object.c in the Linux kernel through 4.11.8 allows attackers to cause a denial of service (memory consumption) by triggering object-initialization failures.
CVE-2017-10911	The make_response function in drivers/block/xen-blkback/blkback.c in the Linux kernel before 4.11.8

	allows guest OS users to obtain sensitive information from host OS (or other guest OS) kernel memory by leveraging the copying of uninitialized padding fields in Xen block-interface response structures, aka XSA-216.
CVE-2017-10928	In ImageMagick 7.0.6-0, a heap-based buffer over-read in the GetNextToken function in token.c allows remote attackers to obtain sensitive information from process memory or possibly have unspecified other impact via a crafted SVG document that is mishandled in the GetUserSpaceCoordinateValue function in coders/svg.c.
CVE-2017-10965	An issue was discovered in Irssi before 1.0.4. When receiving messages with invalid time stamps, Irssi would try to dereference a NULL pointer.
CVE-2017-10966	An issue was discovered in Irssi before 1.0.4. While updating the internal nick list, Irssi could incorrectly use the GHashTable interface and free the nick while updating it. This would then result in use-after-free conditions on each access of the hash table.
CVE-2017-10971	In the X.Org X server before 2017-06-19, a user authenticated to an X Session could crash or execute code in the context of the X Server by exploiting a stack overflow in the endianness conversion of X Events.
CVE-2017-10972	Uninitialized data in endianness conversion in the XEvent handling of the X.Org X Server before 2017-06-19 allowed authenticated malicious users to access potentially privileged data from the X server.
CVE-2017-10978	An FR-GV-201 issue in FreeRADIUS 2.x before 2.2.10 and 3.x before 3.0.15 allows "Read / write overflow in make_secret()" and a denial of service.
CVE-2017-10979	An FR-GV-202 issue in FreeRADIUS 2.x before 2.2.10 allows "Write overflow in rad_coalesce()" - this allows remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code.
CVE-2017-10980	An FR-GV-203 issue in FreeRADIUS 2.x before 2.2.10 allows "DHCP - Memory leak in decode_tlv()" and a denial of service.
CVE-2017-10981	An FR-GV-204 issue in FreeRADIUS 2.x before 2.2.10 allows "DHCP - Memory leak in fr_dhcp_decode()" and a denial of service.
CVE-2017-10982	An FR-GV-205 issue in FreeRADIUS 2.x before 2.2.10 allows "DHCP - Buffer over-read in fr_dhcp_decode_options()" and a denial of service.
CVE-2017-10983	An FR-GV-206 issue in FreeRADIUS 2.x before 2.2.10 and 3.x before 3.0.15 allows "DHCP - Read overflow when decoding option 63" and a denial of service.
CVE-2017-10984	An FR-GV-301 issue in FreeRADIUS 3.x before 3.0.15 allows "Write overflow in data2vp_wimax()" - this allows

	remote attackers to cause a denial of service (daemon crash) or possibly execute arbitrary code.
CVE-2017-10985	An FR-GV-302 issue in FreeRADIUS 3.x before 3.0.15 allows "Infinite loop and memory exhaustion with 'concat' attributes" and a denial of service.
CVE-2017-10986	An FR-GV-303 issue in FreeRADIUS 3.x before 3.0.15 allows "DHCP - Infinite read in dhcp_attr2vp()" and a denial of service.
CVE-2017-10987	An FR-GV-304 issue in FreeRADIUS 3.x before 3.0.15 allows "DHCP - Buffer over-read in fr_dhcp_decode_suboptions()" and a denial of service.
CVE-2017-10995	The mng_get_long function in coders/png.c in ImageMagick 7.0.6-0 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted MNG image.
CVE-2017-11103	Heimdal before 7.4 allows remote attackers to impersonate services with Orpheus' Lyre attacks because it obtains service-principal names in a way that violates the Kerberos 5 protocol specification. In _krb5_extract_ticket() the KDC-REP service name must be obtained from the encrypted version stored in 'enc_part' instead of the unencrypted version stored in 'ticket'. Use of the unencrypted version provides an opportunity for successful server impersonation and other attacks. NOTE: this CVE is only for Heimdal and other products that embed Heimdal code; it does not apply to other instances in which this part of the Kerberos 5 protocol specification is violated.
CVE-2017-11108	tcpdump 4.9.0 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via crafted packet data. The crash occurs in the EXTRACT_16BITS function, called from the stp_print function for the Spanning Tree Protocol.
CVE-2017-11141	The ReadMATImage function in coders\mat.c in ImageMagick 7.0.5-6 has a memory leak vulnerability that can cause memory exhaustion via a crafted MAT file, related to incorrect ordering of a SetImageExtent call.
CVE-2017-11144	In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, the openssl extension PEM sealing code did not check the return value of the OpenSSL sealing function, which could lead to a crash of the PHP interpreter, related to an interpretation conflict for a negative number in ext/openssl/openssl.c, and an OpenSSL documentation omission.
CVE-2017-11145	In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, an error in the date extension's timelib_meridian parsing code could be used by attackers able to supply date strings to leak information from the interpreter, related to ext/date/

	lib/parse_date.c out-of-bounds reads affecting the php_parse_date function. NOTE: the correct fix is in the e8b7698f5ee757ce2c8bd10a192a491a498f891c commit, not the bd77ac90d3bdf31ce2a5251ad92e9e75 gist.
CVE-2017-11170	The ReadTGAImage function in coders\tga.c in ImageMagick 7.0.5-6 has a memory leak vulnerability that can cause memory exhaustion via invalid colors data in the header of a TGA or VST file.
CVE-2017-11176	The mq_notify function in the Linux kernel through 4.11.9 does not set the sock pointer to NULL upon entry into the retry logic. During a user-space close of a Netlink socket, it allows attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact.
CVE-2017-11185	The gmp plugin in strongSwan before 5.6.0 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted RSA signature.
CVE-2017-11188	The ReadDPXImage function in coders\dpx.c in ImageMagick 7.0.6-0 has a large loop vulnerability that can cause CPU exhaustion via a crafted DPX file, related to lack of an EOF check.
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-2017-11334	The address_space_write_continue function in exec.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (out-of-bounds access and guest instance crash) by leveraging use of qemu_map_ram_ptr to access guest ram block area.
CVE-2017-11335	There is a heap based buffer overflow in tools/tiff2pdf.c of LibTIFF 4.0.8 via a PlanarConfig=Contig image, which causes a more than one hundred bytes out-of-bounds write (related to the ZIPDecode function in tif_zip.c). A crafted input may lead to a remote denial of service attack or an arbitrary code execution attack.
CVE-2017-11352	In ImageMagick before 7.0.5-10, a crafted RLE image can trigger a crash because of incorrect EOF handling in coders/rle.c. NOTE: this vulnerability exists because of an incomplete fix for CVE-2017-9144.
CVE-2017-11360	The ReadRLEImage function in coders\rle.c in ImageMagick 7.0.6-1 has a large loop vulnerability via a crafted rle file that triggers a huge number_pixels value.
CVE-2017-11362	In PHP 7.x before 7.0.21 and 7.1.x before 7.1.7, ext/intl/msgformat/msgformat_parse.c does not restrict the locale length, which allows remote attackers to cause a denial of service (stack-based buffer overflow and application crash) or possibly have unspecified other impact within International Components for Unicode (ICU) for C/C++ via a long first argument to the msgfmt_parse_message function.
CVE-2017-11423	The cabd_read_string function in mspack/cabd.c in libmspack 0.5alpha, as used in ClamAV 0.99.2 and other products, allows remote attackers to cause a denial of service (stack-based buffer over-read and application crash) via a crafted CAB file.

CVE-2017-11424	In PyJWT 1.5.0 and below the `invalid_strings` check in `HMACAlgorithm.prepare_key` does not account for all PEM encoded public keys. Specifically, the PKCS1 PEM encoded format would be allowed because it is prefaced with the string `-----BEGIN RSA PUBLIC KEY-----` which is not accounted for. This enables symmetric/asymmetric key confusion attacks against users using the PKCS1 PEM encoded public keys, which would allow an attacker to craft JWTs from scratch.
CVE-2017-11434	The dhcp_decode function in slirp/bootp.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (out-of-bounds read and QEMU process crash) via a crafted DHCP options string.
CVE-2017-11447	The ReadSCREENSHOTImage function in coders/screenshot.c in ImageMagick before 7.0.6-1 has memory leaks, causing denial of service.
CVE-2017-11448	The ReadJPEGImage function in coders/jpeg.c in ImageMagick before 7.0.6-1 allows remote attackers to obtain sensitive information from uninitialized memory locations via a crafted file.
CVE-2017-11449	coders/mpc.c in ImageMagick before 7.0.6-1 does not enable seekable streams and thus cannot validate blob sizes, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an image received from stdin.
CVE-2017-11450	coders/jpeg.c in ImageMagick before 7.0.6-1 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via JPEG data that is too short.
CVE-2017-11472	The acpi_ns_terminate() function in drivers/acpi/acpica/nsutils.c in the Linux kernel before 4.12 does not flush the operand cache and causes a kernel stack dump, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism (in the kernel through 4.9) via a crafted ACPI table.
CVE-2017-11478	The ReadOneDJVUImage function in coders/djvu.c in ImageMagick through 6.9.9-0 and 7.x through 7.0.6-1 allows remote attackers to cause a denial of service (infinite loop and CPU consumption) via a malformed DJVU image.
CVE-2017-11533	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a heap-based buffer over-read in the WriteUILImage() function in coders/uil.c.

CVE-2017-11535	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a heap-based buffer over-read in the WritePSImage() function in coders/ps.c.
CVE-2017-11537	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a Floating Point Exception (FPE) in the WritePALMImage() function in coders/palm.c, related to an incorrect bits-per-pixel calculation.
CVE-2017-11541	tcpdump 4.9.0 has a heap-based buffer over-read in the lldp_print function in print-lldp.c, related to util-print.c.
CVE-2017-11542	tcpdump 4.9.0 has a heap-based buffer over-read in the pimv1_print function in print-pim.c.
CVE-2017-11543	tcpdump 4.9.0 has a buffer overflow in the sliplink_print function in print-sl.c.
CVE-2017-11591	There is a Floating point exception in the Exiv2::ValueType function in Exiv2 0.26 that will lead to a remote denial of service attack via crafted input.
CVE-2017-11613	In LibTIFF 4.0.8, there is a denial of service vulnerability in the TIFFOpen function. A crafted input will lead to a denial of service attack. During the TIFFOpen process, td_imagelength is not checked. The value of td_imagelength can be directly controlled by an input file. In the ChopUpSingleUncompressedStrip function, the _TIFFCheckMalloc function is called based on td_imagelength. If we set the value of td_imagelength close to the amount of system memory, it will hang the system or trigger the OOM killer.
CVE-2017-11624	A stack-consumption vulnerability was found in libqpdf in QPDF 6.0.0, which allows attackers to cause a denial of service via a crafted file, related to the QPDFTokenizer::resolveLiteral function in QPDFTokenizer.cc after two consecutive calls to QPDFObjectHandle::parseInternal, aka an "infinite loop."
CVE-2017-11625	A stack-consumption vulnerability was found in libqpdf in QPDF 6.0.0, which allows attackers to cause a denial of service via a crafted file, related to the QPDF::resolveObjectsInStream function in QPDF.cc, aka an "infinite loop."
CVE-2017-11626	A stack-consumption vulnerability was found in libqpdf in QPDF 6.0.0, which allows attackers to cause a denial of service via a crafted file, related to the QPDFTokenizer::resolveLiteral function in QPDFTokenizer.cc after four consecutive calls to QPDFObjectHandle::parseInternal, aka an "infinite loop."
CVE-2017-11627	A stack-consumption vulnerability was found in libqpdf in QPDF 6.0.0, which allows attackers to cause a denial of service via a crafted file, related to the PointerHolder function in PointerHolder.hh, aka an "infinite loop."

CVE-2017-11628	In PHP before 5.6.31, 7.x before 7.0.21, and 7.1.x before 7.1.7, a stack-based buffer overflow in the zend_ini_do_op() function in Zend/zend_ini_parser.c could cause a denial of service or potentially allow executing code. NOTE: this is only relevant for PHP applications that accept untrusted input (instead of the system's php.ini file) for the parse_ini_string or parse_ini_file function, e.g., a web application for syntax validation of php.ini directives.
CVE-2017-11639	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to a heap-based buffer over-read in the WriteCIPImage() function in coders/cip.c, related to the GetPixelLuma function in MagickCore/pixel-accessor.h.
CVE-2017-11640	When ImageMagick 7.0.6-1 processes a crafted file in convert, it can lead to an address access exception in the WritePTIFImage() function in coders/tiff.c.
CVE-2017-11683	There is a reachable assertion in the Internal::TiffReader::visitDirectory function in tiffvisitor.cpp of Exiv2 0.26 that will lead to a remote denial of service attack via crafted input.
CVE-2017-11714	psi/ztoken.c in Artifex Ghostscript 9.21 mishandles references to the scanner state structure, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PostScript document, related to an out-of-bounds read in the igc_reloc_struct_ptr function in psi/igc.c.
CVE-2017-12134	The xen_biovec_phys_mergeable function in drivers/xen/biomerge.c in Xen might allow local OS guest users to corrupt block device data streams and consequently obtain sensitive memory information, cause a denial of service, or gain host OS privileges by leveraging incorrect block IO merge-ability calculation.
CVE-2017-12140	The ReadDCMImage function in coders\dcm.c in ImageMagick 7.0.6-1 has an integer signedness error leading to excessive memory consumption via a crafted DCM file.
CVE-2017-12146	The driver_override implementation in drivers/base/platform.c in the Linux kernel before 4.12.1 allows local users to gain privileges by leveraging a race condition between a read operation and a store operation that involve different overrides.
CVE-2017-12150	It was found that samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8 did not enforce "SMB signing" when certain configuration options were enabled. A remote attacker could launch a man-in-the-middle attack and retrieve information in plain-text.
CVE-2017-12151	A flaw was found in the way samba client before samba 4.4.16, samba 4.5.14 and samba 4.6.8 used encryption

	with the max protocol set as SMB3. The connection could lose the requirement for signing and encrypting to any DFS redirects, allowing an attacker to read or alter the contents of the connection via a man-in-the-middle attack.
CVE-2017-12153	A security flaw was discovered in the nl80211_set_rekey_data() function in net/wireless/nl80211.c in the Linux kernel through 4.13.3. This function does not check whether the required attributes are present in a Netlink request. This request can be issued by a user with the CAP_NET_ADMIN capability and may result in a NULL pointer dereference and system crash.
CVE-2017-12154	The prepare_vmcs02 function in arch/x86/kvm/vmx.c in the Linux kernel through 4.13.3 does not ensure that the "CR8-load exiting" and "CR8-store exiting" L0 vmcs02 controls exist in cases where L1 omits the "use TPR shadow" vmcs12 control, which allows KVM L2 guest OS users to obtain read and write access to the hardware CR8 register.
CVE-2017-12163	An information leak flaw was found in the way SMB1 protocol was implemented by Samba before 4.4.16, 4.5.x before 4.5.14, and 4.6.x before 4.6.8. A malicious client could use this flaw to dump server memory contents to a file on the samba share or to a shared printer, though the exact area of server memory cannot be controlled by the attacker.
CVE-2017-12173	It was found that sssd's sysdb_search_user_by_upn_res() function before 1.16.0 did not sanitize requests when querying its local cache and was vulnerable to injection. In a centralized login environment, if a password hash was locally cached for a given user, an authenticated attacker could use this flaw to retrieve it.
CVE-2017-12176	xorg-x11-server before 1.19.5 was missing extra length validation in ProcEstablishConnection function allowing malicious X client to cause X server to crash or possibly execute arbitrary code.
CVE-2017-12177	xorg-x11-server before 1.19.5 was vulnerable to integer overflow in ProcDbeGetVisualInfo function allowing malicious X client to cause X server to crash or possibly execute arbitrary code.
CVE-2017-12178	xorg-x11-server before 1.19.5 had wrong extra length check in ProcXIChangeHierarchy function allowing malicious X client to cause X server to crash or possibly execute arbitrary code.
CVE-2017-12179	xorg-x11-server before 1.19.5 was vulnerable to integer overflow in (S)ProcXIBarrierReleasePointer functions allowing malicious X client to cause X server to crash or possibly execute arbitrary code.

CVE-2017-12180	xorg-x11-server before 1.19.5 was missing length validation in XFree86 VidModeExtension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.
CVE-2017-12181	xorg-x11-server before 1.19.5 was missing length validation in XFree86 DGA extension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.
CVE-2017-12182	xorg-x11-server before 1.19.5 was missing length validation in XFree86 DRI extension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.
CVE-2017-12183	xorg-x11-server before 1.19.5 was missing length validation in XFIXES extension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.
CVE-2017-12184	xorg-x11-server before 1.19.5 was missing length validation in XINERAMA extension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.
CVE-2017-12185	xorg-x11-server before 1.19.5 was missing length validation in MIT-SCREEN-SAVER extension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.
CVE-2017-12186	xorg-x11-server before 1.19.5 was missing length validation in X-Resource extension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.
CVE-2017-12187	xorg-x11-server before 1.19.5 was missing length validation in RENDER extension allowing malicious X client to cause X server to crash or possibly execute arbitrary code.
CVE-2017-12188	arch/x86/kvm/mmu.c in the Linux kernel through 4.13.5, when nested virtualisation is used, does not properly traverse guest pagetable entries to resolve a guest virtual address, which allows L1 guest OS users to execute arbitrary code on the host OS or cause a denial of service (incorrect index during page walking, and host OS crash), aka an "MMU potential stack buffer overrun."
CVE-2017-12190	The bio_map_user_iov and bio_unmap_user functions in block/bio.c in the Linux kernel before 4.13.8 do unbalanced refcounting when a SCSI I/O vector has small consecutive buffers belonging to the same page. The bio_add_pc_page function merges them into one, but the page reference is never dropped. This causes a memory leak and possible system lockup (exploitable against the host OS by a guest OS user, if a SCSI disk

	is passed through to a virtual machine) due to an out-of-memory condition.
CVE-2017-12192	The keyctl_read_key function in security/keys/keyctl.c in the Key Management subcomponent in the Linux kernel before 4.13.5 does not properly consider that a key may be possessed but negatively instantiated, which allows local users to cause a denial of service (OOPS and system crash) via a crafted KEYCTL_READ operation.
CVE-2017-12193	The assoc_array_insert_into_terminal_node function in lib/assoc_array.c in the Linux kernel before 4.13.11 mishandles node splitting, which allows local users to cause a denial of service (NULL pointer dereference and panic) via a crafted application, as demonstrated by the keyring key type, and key addition and link creation operations.
CVE-2017-12194	A flaw was found in the way spice-client processed certain messages sent from the server. An attacker, having control of malicious spice-server, could use this flaw to crash the client or execute arbitrary code with permissions of the user running the client. spice-gtk versions through 0.34 are believed to be vulnerable.
CVE-2017-12374	The ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a lack of input validation checking mechanisms during certain mail parsing operations (mbox.c operations on bounce messages). If successfully exploited, the ClamAV software could allow a variable pointing to the mail body which could cause a used after being free (use-after-free) instance which may lead to a disruption of services on an affected device to include a denial of service condition.
CVE-2017-12375	The ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to a lack of input validation checking mechanisms during certain mail parsing functions (the rfc2047 function in mbox.c). An unauthenticated, remote attacker could exploit this vulnerability by sending a crafted email to the affected device. This action could cause a buffer overflow condition when ClamAV scans the malicious email, allowing the attacker to potentially cause a DoS condition on an affected device.
CVE-2017-12376	ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or potentially execute arbitrary code on an affected device. The vulnerability is due

	to improper input validation checking mechanisms when handling Portable Document Format (.pdf) files sent to an affected device. An unauthenticated, remote attacker could exploit this vulnerability by sending a crafted .pdf file to an affected device. This action could cause a handle_pdfname (in pdf.c) buffer overflow when ClamAV scans the malicious file, allowing the attacker to cause a DoS condition or potentially execute arbitrary code.
CVE-2017-12377	ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or potentially execute arbitrary code on an affected device. The vulnerability is due to improper input validation checking mechanisms in mew packet files sent to an affected device. A successful exploit could cause a heap-based buffer over-read condition in mew.c when ClamAV scans the malicious file, allowing the attacker to cause a DoS condition or potentially execute arbitrary code on the affected device.
CVE-2017-12378	ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper input validation checking mechanisms of .tar (Tape Archive) files sent to an affected device. A successful exploit could cause a checksum buffer over-read condition when ClamAV scans the malicious .tar file, potentially allowing the attacker to cause a DoS condition on the affected device.
CVE-2017-12379	ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition or potentially execute arbitrary code on an affected device. The vulnerability is due to improper input validation checking mechanisms in the message parsing function on an affected system. An unauthenticated, remote attacker could exploit this vulnerability by sending a crafted email to the affected device. This action could cause a messageAddArgument (in message.c) buffer overflow condition when ClamAV scans the malicious email, allowing the attacker to potentially cause a DoS condition or execute arbitrary code on an affected device.
CVE-2017-12380	ClamAV AntiVirus software versions 0.99.2 and prior contain a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper input validation checking

	mechanisms in mbox.c during certain mail parsing functions of the ClamAV software. An unauthenticated, remote attacker could exploit this vulnerability by sending a crafted email to the affected device. An exploit could trigger a NULL pointer dereference condition when ClamAV scans the malicious email, which may result in a DoS condition.
CVE-2017-12418	ImageMagick 7.0.6-5 has memory leaks in the parse8BIMW and format8BIM functions in coders/meta.c, related to the WriteImage function in MagickCore/constitute.c.
CVE-2017-12429	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadMIFFImage in coders/miff.c, which allows attackers to cause a denial of service.
CVE-2017-12430	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadMPCImage in coders/mpc.c, which allows attackers to cause a denial of service.
CVE-2017-12431	In ImageMagick 7.0.6-1, a use-after-free vulnerability was found in the function ReadWMFImage in coders/wmf.c, which allows attackers to cause a denial of service.
CVE-2017-12432	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadPCXImage in coders/pcx.c, which allows attackers to cause a denial of service.
CVE-2017-12433	In ImageMagick 7.0.6-1, a memory leak vulnerability was found in the function ReadPESImage in coders/pes.c, which allows attackers to cause a denial of service, related to ResizeMagickMemory in memory.c.
CVE-2017-12435	In ImageMagick 7.0.6-1, a memory exhaustion vulnerability was found in the function ReadSUNImage in coders/sun.c, which allows attackers to cause a denial of service.
CVE-2017-12563	In ImageMagick 7.0.6-2, a memory exhaustion vulnerability was found in the function ReadPSDImage in coders/psd.c, which allows attackers to cause a denial of service.
CVE-2017-12587	ImageMagick 7.0.6-1 has a large loop vulnerability in the ReadPWPImage function in coders\pwp.c.
CVE-2017-12595	The tokenizer in QPDF 6.0.0 and 7.0.b1 is recursive for arrays and dictionaries, which allows remote attackers to cause a denial of service (stack consumption and segmentation fault) or possibly have unspecified other impact via a PDF document with a deep data structure, as demonstrated by a crash in QPDFObjectHandle::parseInternal in libqpdf/QPDFObjectHandle.cc.

CVE-2017-12616	When using a VirtualDirContext with Apache Tomcat 7.0.0 to 7.0.80 it was possible to bypass security constraints and/or view the source code of JSPs for resources served by the VirtualDirContext using a specially crafted request.
CVE-2017-12617	When running Apache Tomcat versions 9.0.0.M1 to 9.0.0, 8.5.0 to 8.5.22, 8.0.0.RC1 to 8.0.46 and 7.0.0 to 7.0.81 with HTTP PUTs enabled (e.g. via setting the readonly initialisation parameter of the Default servlet to false) it was possible to upload a JSP file to the server via a specially crafted request. This JSP could then be requested and any code it contained would be executed by the server.
CVE-2017-12629	Remote code execution occurs in Apache Solr before 7.1 with Apache Lucene before 7.1 by exploiting XXE in conjunction with use of a Config API add-listener command to reach the RunExecutableListener class. Elasticsearch, although it uses Lucene, is NOT vulnerable to this. Note that the XML external entity expansion vulnerability occurs in the XML Query Parser which is available, by default, for any query request with parameters deftype=xmlparser and can be exploited to upload malicious data to the /upload request handler or as Blind XXE using ftp wrapper in order to read arbitrary local files from the Solr server. Note also that the second vulnerability relates to remote code execution using the RunExecutableListener available on all affected versions of Solr.
CVE-2017-12640	ImageMagick 7.0.6-1 has an out-of-bounds read vulnerability in ReadOneMNGImage in coders/png.c.
CVE-2017-12643	ImageMagick 7.0.6-1 has a memory exhaustion vulnerability in ReadOneJNGImage in coders\png.c.
CVE-2017-12644	ImageMagick 7.0.6-1 has a memory leak vulnerability in ReadDCMImage in coders\dcm.c.
CVE-2017-12670	In ImageMagick 7.0.6-3, missing validation was found in coders/mat.c, leading to an assertion failure in the function DestroyImage in MagickCore/image.c, which allows attackers to cause a denial of service.
CVE-2017-12674	In ImageMagick 7.0.6-2, a CPU exhaustion vulnerability was found in the function ReadPDBImage in coders/pdb.c, which allows attackers to cause a denial of service.
CVE-2017-12691	The ReadOneLayer function in coders/xcf.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted file.
CVE-2017-12692	The ReadVIFFImage function in coders/viff.c in ImageMagick 7.0.6-6 allows remote attackers to cause

	a denial of service (memory consumption) via a crafted VIFF file.
CVE-2017-12693	The ReadBMPImage function in coders/bmp.c in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (memory consumption) via a crafted BMP file.
CVE-2017-12762	In /drivers/isdn/i4l/isdn_net.c: A user-controlled buffer is copied into a local buffer of constant size using strcpy without a length check which can cause a buffer overflow. This affects the Linux kernel 4.9-stable tree, 4.12-stable tree, 3.18-stable tree, and 4.4-stable tree.
CVE-2017-12809	QEMU (aka Quick Emulator), when built with the IDE disk and CD/DVD-ROM Emulator support, allows local guest OS privileged users to cause a denial of service (NULL pointer dereference and QEMU process crash) by flushing an empty CDROM device drive.
CVE-2017-12836	CVS 1.12.x, when configured to use SSH for remote repositories, might allow remote attackers to execute arbitrary code via a repository URL with a crafted hostname, as demonstrated by "-oProxyCommand=id;localhost:/bar."
CVE-2017-12837	Heap-based buffer overflow in the S_regatom function in regcomp.c in Perl 5 before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to cause a denial of service (out-of-bounds write) via a regular expression with a '\N{}' escape and the case-insensitive modifier.
CVE-2017-12875	The WritePixelCachePixels function in ImageMagick 7.0.6-6 allows remote attackers to cause a denial of service (CPU consumption) via a crafted file.
CVE-2017-12877	Use-after-free vulnerability in the DestroyImage function in image.c in ImageMagick before 7.0.6-6 allows remote attackers to cause a denial of service via a crafted file.
CVE-2017-12883	Buffer overflow in the S_grok_bslash_N function in regcomp.c in Perl 5 before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to disclose sensitive information or cause a denial of service (application crash) via a crafted regular expression with an invalid '\N{U+...}' escape.
CVE-2017-12893	The SMB/CIFS parser in tcpdump before 4.9.2 has a buffer over-read in smbutil.c:name_len().
CVE-2017-12894	Several protocol parsers in tcpdump before 4.9.2 could cause a buffer over-read in addrtoname.c:lookup_bytestring().
CVE-2017-12895	The ICMP parser in tcpdump before 4.9.2 has a buffer over-read in print-icmp.c:icmp_print().
CVE-2017-12896	The ISAKMP parser in tcpdump before 4.9.2 has a buffer over-read in print-isakmp.c:isakmp_rfc3948_print().

CVE-2017-12897	The ISO CLNS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:isoclns_print().
CVE-2017-12898	The NFS parser in tcpdump before 4.9.2 has a buffer over-read in print-nfs.c:interp_reply().
CVE-2017-12899	The DECnet parser in tcpdump before 4.9.2 has a buffer over-read in print-decnet.c:decnet_print().
CVE-2017-12900	Several protocol parsers in tcpdump before 4.9.2 could cause a buffer over-read in util-print.c:tok2strbuf().
CVE-2017-12901	The EIGRP parser in tcpdump before 4.9.2 has a buffer over-read in print-eigrp.c:eigrp_print().
CVE-2017-12902	The Zephyr parser in tcpdump before 4.9.2 has a buffer over-read in print-zephyr.c, several functions.
CVE-2017-12944	The TIFFReadDirEntryArray function in tif_read.c in LibTIFF 4.0.8 mishandles memory allocation for short files, which allows remote attackers to cause a denial of service (allocation failure and application crash) in the TIFFFetchStripThing function in tif_dirread.c during a tiff2pdf invocation.
CVE-2017-12983	Heap-based buffer overflow in the ReadSFWImage function in coders/sfw.c in ImageMagick 7.0.6-8 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file.
CVE-2017-12985	The IPv6 parser in tcpdump before 4.9.2 has a buffer over-read in print-ip6.c:ip6_print().
CVE-2017-12986	The IPv6 routing header parser in tcpdump before 4.9.2 has a buffer over-read in print-rt6.c:rt6_print().
CVE-2017-12987	The IEEE 802.11 parser in tcpdump before 4.9.2 has a buffer over-read in print-802_11.c:parse_elements().
CVE-2017-12988	The telnet parser in tcpdump before 4.9.2 has a buffer over-read in print-telnet.c:telnet_parse().
CVE-2017-12989	The RESP parser in tcpdump before 4.9.2 could enter an infinite loop due to a bug in print-resp.c:resp_get_length().
CVE-2017-12990	The ISAKMP parser in tcpdump before 4.9.2 could enter an infinite loop due to bugs in print-isakmp.c, several functions.
CVE-2017-12991	The BGP parser in tcpdump before 4.9.2 has a buffer over-read in print-bgp.c:bgp_attr_print().
CVE-2017-12992	The RIPng parser in tcpdump before 4.9.2 has a buffer over-read in print-ripng.c:ripng_print().
CVE-2017-12993	The Juniper protocols parser in tcpdump before 4.9.2 has a buffer over-read in print-juniper.c, several functions.
CVE-2017-12994	The BGP parser in tcpdump before 4.9.2 has a buffer over-read in print-bgp.c:bgp_attr_print().

CVE-2017-12995	The DNS parser in tcpdump before 4.9.2 could enter an infinite loop due to a bug in print-domain.c:ns_print().
CVE-2017-12996	The PIMv2 parser in tcpdump before 4.9.2 has a buffer over-read in print-pim.c:pimv2_print().
CVE-2017-12997	The LLDP parser in tcpdump before 4.9.2 could enter an infinite loop due to a bug in print-lldp.c:lldp_private_8021_print().
CVE-2017-12998	The IS-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:isis_print_extd_ip_reach().
CVE-2017-12999	The IS-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:isis_print().
CVE-2017-13000	The IEEE 802.15.4 parser in tcpdump before 4.9.2 has a buffer over-read in print-802_15_4.c:ieee802_15_4_if_print().
CVE-2017-13001	The NFS parser in tcpdump before 4.9.2 has a buffer over-read in print-nfs.c:nfs_printfh().
CVE-2017-13002	The AODV parser in tcpdump before 4.9.2 has a buffer over-read in print-aodv.c:aodv_extension().
CVE-2017-13003	The LMP parser in tcpdump before 4.9.2 has a buffer over-read in print-lmp.c:lmp_print().
CVE-2017-13004	The Juniper protocols parser in tcpdump before 4.9.2 has a buffer over-read in print-juniper.c:juniper_parse_header().
CVE-2017-13005	The NFS parser in tcpdump before 4.9.2 has a buffer over-read in print-nfs.c:xid_map_enter().
CVE-2017-13006	The L2TP parser in tcpdump before 4.9.2 has a buffer over-read in print-l2tp.c, several functions.
CVE-2017-13007	The Apple PKTAP parser in tcpdump before 4.9.2 has a buffer over-read in print-pktap.c:pktap_if_print().
CVE-2017-13008	The IEEE 802.11 parser in tcpdump before 4.9.2 has a buffer over-read in print-802_11.c:parse_elements().
CVE-2017-13009	The IPv6 mobility parser in tcpdump before 4.9.2 has a buffer over-read in print-mobility.c:mobility_print().
CVE-2017-13010	The BEEP parser in tcpdump before 4.9.2 has a buffer over-read in print-beep.c:l_strnstart().
CVE-2017-13011	Several protocol parsers in tcpdump before 4.9.2 could cause a buffer overflow in util-print.c:bittok2str_internal().
CVE-2017-13012	The ICMP parser in tcpdump before 4.9.2 has a buffer over-read in print-icmp.c:icmp_print().
CVE-2017-13013	The ARP parser in tcpdump before 4.9.2 has a buffer over-read in print-arp.c, several functions.
CVE-2017-13014	The White Board protocol parser in tcpdump before 4.9.2 has a buffer over-read in print-wb.c:wb_prep(), several functions.

CVE-2017-13015	The EAP parser in tcpdump before 4.9.2 has a buffer over-read in print-eap.c:eap_print().
CVE-2017-13016	The ISO ES-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:esis_print().
CVE-2017-13017	The DHCPv6 parser in tcpdump before 4.9.2 has a buffer over-read in print-dhcp6.c:dhcp6opt_print().
CVE-2017-13018	The PGM parser in tcpdump before 4.9.2 has a buffer over-read in print-pgm.c:pgm_print().
CVE-2017-13019	The PGM parser in tcpdump before 4.9.2 has a buffer over-read in print-pgm.c:pgm_print().
CVE-2017-13020	The VTP parser in tcpdump before 4.9.2 has a buffer over-read in print-vtp.c:vtp_print().
CVE-2017-13021	The ICMPv6 parser in tcpdump before 4.9.2 has a buffer over-read in print-icmp6.c:icmp6_print().
CVE-2017-13022	The IP parser in tcpdump before 4.9.2 has a buffer over-read in print-ip.c:ip_printroute().
CVE-2017-13023	The IPv6 mobility parser in tcpdump before 4.9.2 has a buffer over-read in print-mobility.c:mobility_opt_print().
CVE-2017-13024	The IPv6 mobility parser in tcpdump before 4.9.2 has a buffer over-read in print-mobility.c:mobility_opt_print().
CVE-2017-13025	The IPv6 mobility parser in tcpdump before 4.9.2 has a buffer over-read in print-mobility.c:mobility_opt_print().
CVE-2017-13026	The ISO IS-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c, several functions.
CVE-2017-13027	The LLDP parser in tcpdump before 4.9.2 has a buffer over-read in print-lldp.c:lldp_mgmt_addr_tlv_print().
CVE-2017-13028	The BOOTP parser in tcpdump before 4.9.2 has a buffer over-read in print-bootp.c:bootp_print().
CVE-2017-13029	The PPP parser in tcpdump before 4.9.2 has a buffer over-read in print-ppp.c:print_ccp_config_options().
CVE-2017-13030	The PIM parser in tcpdump before 4.9.2 has a buffer over-read in print-pim.c, several functions.
CVE-2017-13031	The IPv6 fragmentation header parser in tcpdump before 4.9.2 has a buffer over-read in print-frag6.c:frag6_print().
CVE-2017-13032	The RADIUS parser in tcpdump before 4.9.2 has a buffer over-read in print-radius.c:print_attr_string().
CVE-2017-13033	The VTP parser in tcpdump before 4.9.2 has a buffer over-read in print-vtp.c:vtp_print().
CVE-2017-13034	The PGM parser in tcpdump before 4.9.2 has a buffer over-read in print-pgm.c:pgm_print().
CVE-2017-13035	The ISO IS-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:isis_print_id().
CVE-2017-13036	The OSPFv3 parser in tcpdump before 4.9.2 has a buffer over-read in print-ospf6.c:ospf6_decode_v3().

CVE-2017-13037	The IP parser in tcpdump before 4.9.2 has a buffer over-read in print-ip.c:ip_printts().
CVE-2017-13038	The PPP parser in tcpdump before 4.9.2 has a buffer over-read in print-ppp.c:handle_mlppp().
CVE-2017-13039	The ISAKMP parser in tcpdump before 4.9.2 has a buffer over-read in print-isakmp.c, several functions.
CVE-2017-13040	The MPTCP parser in tcpdump before 4.9.2 has a buffer over-read in print-mptcp.c, several functions.
CVE-2017-13041	The ICMPv6 parser in tcpdump before 4.9.2 has a buffer over-read in print-icmp6.c:icmp6_nodeinfo_print().
CVE-2017-13042	The HNCP parser in tcpdump before 4.9.2 has a buffer over-read in print-hncp.c:dhcpv6_print().
CVE-2017-13043	The BGP parser in tcpdump before 4.9.2 has a buffer over-read in print-bgp.c:decode_multicast_vpn().
CVE-2017-13044	The HNCP parser in tcpdump before 4.9.2 has a buffer over-read in print-hncp.c:dhcpv4_print().
CVE-2017-13045	The VQP parser in tcpdump before 4.9.2 has a buffer over-read in print-vqp.c:vqp_print().
CVE-2017-13046	The BGP parser in tcpdump before 4.9.2 has a buffer over-read in print-bgp.c:bgp_attr_print().
CVE-2017-13047	The ISO ES-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:esis_print().
CVE-2017-13048	The RSVP parser in tcpdump before 4.9.2 has a buffer over-read in print-rsvp.c:rsvp_obj_print().
CVE-2017-13049	The Rx protocol parser in tcpdump before 4.9.2 has a buffer over-read in print-rx.c:ubik_print().
CVE-2017-13050	The RPKI-Router parser in tcpdump before 4.9.2 has a buffer over-read in print-rpki-rtr.c:rpki_rtr_pdu_print().
CVE-2017-13051	The RSVP parser in tcpdump before 4.9.2 has a buffer over-read in print-rsvp.c:rsvp_obj_print().
CVE-2017-13052	The CFM parser in tcpdump before 4.9.2 has a buffer over-read in print-cfm.c:cfm_print().
CVE-2017-13053	The BGP parser in tcpdump before 4.9.2 has a buffer over-read in print-bgp.c:decode_rt_routing_info().
CVE-2017-13054	The LLDP parser in tcpdump before 4.9.2 has a buffer over-read in print-lldp.c:lldp_private_8023_print().
CVE-2017-13055	The ISO IS-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:isis_print_is_reach_subtlv().
CVE-2017-13058	In ImageMagick 7.0.6-6, a memory leak vulnerability was found in the function WritePCXImage in coders/pcx.c, which allows attackers to cause a denial of service via a crafted file.
CVE-2017-13059	In ImageMagick 7.0.6-6, a memory leak vulnerability was found in the function WriteOneJNGImage in

	coders/png.c, which allows attackers to cause a denial of service (WriteJNGImage memory consumption) via a crafted file.
CVE-2017-13060	In ImageMagick 7.0.6-5, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service via a crafted file.
CVE-2017-13061	In ImageMagick 7.0.6-5, a length-validation vulnerability was found in the function ReadPSDLayersInternal in coders/psd.c, which allows attackers to cause a denial of service (ReadPSDImage memory exhaustion) via a crafted file.
CVE-2017-13062	In ImageMagick 7.0.6-6, a memory leak vulnerability was found in the function formatIPTC in coders/meta.c, which allows attackers to cause a denial of service (WriteMETAImage memory consumption) via a crafted file.
CVE-2017-13077	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Pairwise Transient Key (PTK) Temporal Key (TK) during the four-way handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.
CVE-2017-13078	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group Temporal Key (GTK) during the four-way handshake, allowing an attacker within radio range to replay frames from access points to clients.
CVE-2017-13079	Wi-Fi Protected Access (WPA and WPA2) that supports IEEE 802.11w allows reinstallation of the Integrity Group Temporal Key (IGTK) during the four-way handshake, allowing an attacker within radio range to spoof frames from access points to clients.
CVE-2017-13080	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group Temporal Key (GTK) during the group key handshake, allowing an attacker within radio range to replay frames from access points to clients.
CVE-2017-13081	Wi-Fi Protected Access (WPA and WPA2) that supports IEEE 802.11w allows reinstallation of the Integrity Group Temporal Key (IGTK) during the group key handshake, allowing an attacker within radio range to spoof frames from access points to clients.
CVE-2017-13082	Wi-Fi Protected Access (WPA and WPA2) that supports IEEE 802.11r allows reinstallation of the Pairwise Transient Key (PTK) Temporal Key (TK) during the fast BSS transmission (FT) handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.
CVE-2017-13086	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Tunneled Direct-Link Setup (TDLS)

	Peer Key (TPK) during the TDLS handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.
CVE-2017-13087	Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation of the Group Temporal Key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame, allowing an attacker within radio range to replay frames from access points to clients.
CVE-2017-13088	Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation of the Integrity Group Temporal Key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame, allowing an attacker within radio range to replay frames from access points to clients.
CVE-2017-13089	The http.c:skip_short_body() function is called in some circumstances, such as when processing redirects. When the response is sent chunked in wget before 1.19.2, the chunk parser uses strtol() to read each chunk's length, but doesn't check that the chunk length is a non-negative number. The code then tries to skip the chunk in pieces of 512 bytes by using the MIN() macro, but ends up passing the negative chunk length to connect.c:fd_read(). As fd_read() takes an int argument, the high 32 bits of the chunk length are discarded, leaving fd_read() with a completely attacker controlled length argument.
CVE-2017-13090	The retr.c:fd_read_body() function is called when processing OK responses. When the response is sent chunked in wget before 1.19.2, the chunk parser uses strtol() to read each chunk's length, but doesn't check that the chunk length is a non-negative number. The code then tries to read the chunk in pieces of 8192 bytes by using the MIN() macro, but ends up passing the negative chunk length to retr.c:fd_read(). As fd_read() takes an int argument, the high 32 bits of the chunk length are discarded, leaving fd_read() with a completely attacker controlled length argument. The attacker can corrupt malloc metadata after the allocated buffer.
CVE-2017-13131	In ImageMagick 7.0.6-8, a memory leak vulnerability was found in the function ReadMIFFImage in coders/miff.c, which allows attackers to cause a denial of service (memory consumption in NewLinkedList in MagickCore/linked-list.c) via a crafted file.
CVE-2017-13134	In ImageMagick 7.0.6-6 and GraphicsMagick 1.3.26, a heap-based buffer over-read was found in the function SFWScan in coders/sfw.c, which allows attackers to cause a denial of service via a crafted file.

CVE-2017-13139	In ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1, the ReadOneMNGImage function in coders/png.c has an out-of-bounds read with the MNG CLIP chunk.
CVE-2017-13142	In ImageMagick before 6.9.9-0 and 7.x before 7.0.6-1, a crafted PNG file could trigger a crash because there was an insufficient check for short files.
CVE-2017-13143	In ImageMagick before 6.9.7-6 and 7.x before 7.0.4-6, the ReadMATImage function in coders/mat.c uses uninitialized data, which might allow remote attackers to obtain sensitive information from process memory.
CVE-2017-13144	In ImageMagick before 6.9.7-10, there is a crash (rather than a "width or height exceeds limit" error report) if the image dimensions are too large, as demonstrated by use of the mpc coder.
CVE-2017-13145	In ImageMagick before 6.9.8-8 and 7.x before 7.0.5-9, the ReadJP2Image function in coders/jp2.c does not properly validate the channel geometry, leading to a crash.
CVE-2017-13168	An elevation of privilege vulnerability in the kernel scsi driver. Product: Android. Versions: Android kernel. Android ID A-65023233.
CVE-2017-13305	A information disclosure vulnerability in the Upstream kernel encrypted-keys. Product: Android. Versions: Android kernel. Android ID: A-70526974.
CVE-2017-13687	The Cisco HDLC parser in tcpdump before 4.9.2 has a buffer over-read in print-chdlc.c:chdlc_print().
CVE-2017-13688	The OLSR parser in tcpdump before 4.9.2 has a buffer over-read in print-olsr.c:olsr_print().
CVE-2017-13689	The IKEv1 parser in tcpdump before 4.9.2 has a buffer over-read in print-isakmp.c:ikev1_id_print().
CVE-2017-13690	The IKEv2 parser in tcpdump before 4.9.2 has a buffer over-read in print-isakmp.c, several functions.
CVE-2017-13695	The acpi_ns_evaluate() function in drivers/acpi/acpica/nseval.c in the Linux kernel through 4.12.9 does not flush the operand cache and causes a kernel stack dump, which allows local users to obtain sensitive information from kernel memory and bypass the KASLR protection mechanism (in the kernel through 4.9) via a crafted ACPI table.
CVE-2017-13720	In the PatternMatch function in fontfile/fontdir.c in libXfont through 1.5.2 and 2.x before 2.0.2, an attacker with access to an X connection can cause a buffer over-read during pattern matching of fonts, leading to information disclosure or a crash (denial of service). This occurs because '\0' characters are incorrectly skipped in situations involving ? characters.
CVE-2017-13721	In X.Org Server (aka xserver and xorg-server) before 1.19.4, an attacker authenticated to an X server with the

	X shared memory extension enabled can cause aborts of the X server or replace shared memory segments of other X clients in the same session.
CVE-2017-13722	In the pcfGetProperties function in bitmap/pcfread.c in libXfont through 1.5.2 and 2.x before 2.0.2, a missing boundary check (for PCF files) could be used by local attackers authenticated to an Xserver for a buffer over-read, for information disclosure or a crash of the X server.
CVE-2017-13723	In X.Org Server (aka xserver and xorg-server) before 1.19.4, a local attacker authenticated to the X server could overflow a global buffer, causing crashes of the X server or potentially other problems by injecting large or malformed XKB related atoms and accessing them via xkbcomp.
CVE-2017-13725	The IPv6 routing header parser in tcpdump before 4.9.2 has a buffer over-read in print-rt6.c:rt6_print().
CVE-2017-13726	There is a reachable assertion abort in the function TIFFWriteDirectorySec() in LibTIFF 4.0.8, related to tif_dirwrite.c and a SubIFD tag. A crafted input will lead to a remote denial of service attack.
CVE-2017-13727	There is a reachable assertion abort in the function TIFFWriteDirectoryTagSubifd() in LibTIFF 4.0.8, related to tif_dirwrite.c and a SubIFD tag. A crafted input will lead to a remote denial of service attack.
CVE-2017-13735	There is a floating point exception in the kodak_radc_load_raw function in dcraw_common.cpp in LibRaw 0.18.2. It will lead to a remote denial of service attack.
CVE-2017-13738	There is an illegal address access in the _lou_getALine function in compileTranslationTable.c:346 in Liblouis 3.2.0.
CVE-2017-13739	There is a heap-based buffer overflow that causes a more than two thousand bytes out-of-bounds write in Liblouis 3.2.0, triggered in the function resolveSubtable() in compileTranslationTable.c. It will lead to denial of service or remote code execution.
CVE-2017-13740	There is a stack-based buffer overflow in Liblouis 3.2.0, triggered in the function parseChars() in compileTranslationTable.c, that will lead to denial of service or possibly unspecified other impact.
CVE-2017-13742	There is a stack-based buffer overflow in Liblouis 3.2.0, triggered in the function includeFile() in compileTranslationTable.c, that will lead to a remote denial of service attack.
CVE-2017-13744	There is an illegal address access in the function _lou_getALine() in compileTranslationTable.c:343 in Liblouis 3.2.0.

CVE-2017-13758	In ImageMagick 7.0.6-10, there is a heap-based buffer overflow in the TracePoint() function in MagickCore/draw.c.
CVE-2017-13768	Null Pointer Dereference in the IdentifyImage function in MagickCore/identify.c in ImageMagick through 7.0.6-10 allows an attacker to perform denial of service by sending a crafted image file.
CVE-2017-13769	The WriteTHUMBNAILImage function in coders/thumbnail.c in ImageMagick through 7.0.6-10 allows an attacker to cause a denial of service (buffer over-read) by sending a crafted JPEG file.
CVE-2017-13783	An issue was discovered in certain Apple products. iOS before 11.1 is affected. Safari before 11.0.1 is affected. iCloud before 7.1 on Windows is affected. iTunes before 12.7.1 on Windows is affected. tvOS before 11.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13784	An issue was discovered in certain Apple products. iOS before 11.1 is affected. Safari before 11.0.1 is affected. iCloud before 7.1 on Windows is affected. iTunes before 12.7.1 on Windows is affected. tvOS before 11.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13785	An issue was discovered in certain Apple products. iOS before 11.1 is affected. Safari before 11.0.1 is affected. iCloud before 7.1 on Windows is affected. iTunes before 12.7.1 on Windows is affected. tvOS before 11.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13788	An issue was discovered in certain Apple products. iOS before 11.1 is affected. Safari before 11.0.1 is affected. iCloud before 7.1 on Windows is affected. iTunes before 12.7.1 on Windows is affected. tvOS before 11.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13791	An issue was discovered in certain Apple products. iOS before 11.1 is affected. Safari before 11.0.1 is affected. iCloud before 7.1 on Windows is affected. iTunes before 12.7.1 on Windows is affected. tvOS before 11.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code

	or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13792	An issue was discovered in certain Apple products. iOS before 11.1 is affected. Safari before 11.0.1 is affected. iCloud before 7.1 on Windows is affected. iTunes before 12.7.1 on Windows is affected. tvOS before 11.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13793	An issue was discovered in certain Apple products. iOS before 11.1 is affected. Safari before 11.0.1 is affected. iCloud before 7.1 on Windows is affected. iTunes before 12.7.1 on Windows is affected. tvOS before 11.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13794	An issue was discovered in certain Apple products. iOS before 11.1 is affected. Safari before 11.0.1 is affected. iCloud before 7.1 on Windows is affected. iTunes before 12.7.1 on Windows is affected. tvOS before 11.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13795	An issue was discovered in certain Apple products. iOS before 11.1 is affected. Safari before 11.0.1 is affected. iCloud before 7.1 on Windows is affected. iTunes before 12.7.1 on Windows is affected. tvOS before 11.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13796	An issue was discovered in certain Apple products. iOS before 11.1 is affected. Safari before 11.0.1 is affected. iCloud before 7.1 on Windows is affected. iTunes before 12.7.1 on Windows is affected. tvOS before 11.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13798	An issue was discovered in certain Apple products. iOS before 11.1 is affected. Safari before 11.0.1 is affected. iCloud before 7.1 on Windows is affected. iTunes before 12.7.1 on Windows is affected. tvOS before 11.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-13802	An issue was discovered in certain Apple products. iOS before 11.1 is affected. Safari before 11.0.1 is affected. iCloud before 7.1 on Windows is affected. iTunes before 12.7.1 on Windows is affected. tvOS before 11.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13803	An issue was discovered in certain Apple products. iOS before 11.1 is affected. Safari before 11.0.1 is affected. iCloud before 7.1 on Windows is affected. iTunes before 12.7.1 on Windows is affected. tvOS before 11.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13856	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13866	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13870	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13884	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-13885	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected.

	iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-14033	The decode method in the OpenSSL::ASN1 module in Ruby before 2.2.8, 2.3.x before 2.3.5, and 2.4.x through 2.4.1 allows attackers to cause a denial of service (interpreter crash) via a crafted string.
CVE-2017-14051	An integer overflow in the qla2x00_sysfs_write_optrom_ctl function in drivers/scsi/qla2xxx/qla_attr.c in the Linux kernel through 4.12.10 allows local users to cause a denial of service (memory corruption and system crash) by leveraging root access.
CVE-2017-14060	In ImageMagick 7.0.6-10, a NULL Pointer Dereference issue is present in the ReadCUTImage function in coders/cut.c that could allow an attacker to cause a Denial of Service (in the QueueAuthenticPixelCacheNexus function within the MagickCore/cache.c file) by submitting a malformed image file.
CVE-2017-14062	Integer overflow in the decode_digit function in puny_decode.c in Libidn2 before 2.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact.
CVE-2017-14064	Ruby through 2.2.7, 2.3.x through 2.3.4, and 2.4.x through 2.4.1 can expose arbitrary memory during a JSON.generate call. The issues lies in using strdup in ext/json/ext/generator/generator.c, which will stop after encountering a '\0' byte, returning a pointer to a string of length zero, which is not the length stored in space_len.
CVE-2017-14106	The tcp_disconnect function in net/ipv4/tcp.c in the Linux kernel before 4.12 allows local users to cause a denial of service (__tcp_select_window divide-by-zero error and system crash) by triggering a disconnect within a certain tcp_recvmsg code path.
CVE-2017-14140	The move_pages system call in mm/migrate.c in the Linux kernel before 4.12.9 doesn't check the effective uid of the target process, enabling a local attacker to learn the memory layout of a setuid executable despite ASLR.
CVE-2017-14156	The atyfb_ioctl function in drivers/video/fbdev/aty/atyfb_base.c in the Linux kernel through 4.12.10 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory by reading locations associated with padding bytes.
CVE-2017-14166	libarchive 3.3.2 allows remote attackers to cause a denial of service (xml_data heap-based buffer over-

	read and application crash) via a crafted xar archive, related to the mishandling of empty strings in the atol8 function in archive_read_support_format_xar.c.
CVE-2017-14167	Integer overflow in the load_multiboot function in hw/i386/multiboot.c in QEMU (aka Quick Emulator) allows local guest OS users to execute arbitrary code on the host via crafted multiboot header address values, which trigger an out-of-bounds write.
CVE-2017-14172	In coders/ps.c in ImageMagick 7.0.7-0 Q16, a DoS in ReadPSImage() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted PSD file, which claims a large "extent" field in the header but does not contain sufficient backing data, is provided, the loop over "length" would consume huge CPU resources, since there is no EOF check inside the loop.
CVE-2017-14173	In the function ReadTXTImage() in coders/txt.c in ImageMagick 7.0.6-10, an integer overflow might occur for the addition operation "GetQuantumRange(depth)+1" when "depth" is large, producing a smaller value than expected. As a result, an infinite loop would occur for a crafted TXT file that claims a very large "max_value" value.
CVE-2017-14174	In coders/psd.c in ImageMagick 7.0.7-0 Q16, a DoS in ReadPSDLayersInternal() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted PSD file, which claims a large "length" field in the header but does not contain sufficient backing data, is provided, the loop over "length" would consume huge CPU resources, since there is no EOF check inside the loop.
CVE-2017-14175	In coders/xbm.c in ImageMagick 7.0.6-1 Q16, a DoS in ReadXBMImage() due to lack of an EOF (End of File) check might cause huge CPU consumption. When a crafted XBM file, which claims large rows and columns fields in the header but does not contain sufficient backing data, is provided, the loop over the rows would consume huge CPU resources, since there is no EOF check inside the loop.
CVE-2017-14177	Apport through 2.20.7 does not properly handle core dumps from setuid binaries allowing local users to create certain files as root which an attacker could leverage to perform a denial of service via resource exhaustion or possibly gain root privileges. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-1324.
CVE-2017-14180	Apport 2.13 through 2.20.7 does not properly handle crashes originating from a PID namespace allowing local users to create certain files as root which an attacker could leverage to perform a denial of service

	via resource exhaustion or possibly gain root privileges, a different vulnerability than CVE-2017-14179.
CVE-2017-14224	A heap-based buffer overflow in WritePCXImage in coders/pcx.c in ImageMagick 7.0.6-8 Q16 allows remote attackers to cause a denial of service or code execution via a crafted file.
CVE-2017-14249	ImageMagick 7.0.6-8 Q16 mishandles EOF checks in ReadMPCImage in coders/mpc.c, leading to division by zero in GetPixelCacheTileSize in MagickCore/cache.c, allowing remote attackers to cause a denial of service via a crafted file.
CVE-2017-14265	A Stack-based Buffer Overflow was discovered in xtrans_interpolate in internal/dcraw_common.cpp in LibRaw before 0.18.3. It could allow a remote denial of service or code execution attack.
CVE-2017-14325	In ImageMagick 7.0.7-1 Q16, a memory leak vulnerability was found in the function PersistPixelCache in magick/cache.c, which allows attackers to cause a denial of service (memory consumption in ReadMPCImage in coders/mpc.c) via a crafted file.
CVE-2017-14326	In ImageMagick 7.0.7-1 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service via a crafted file.
CVE-2017-14340	The XFS_IS_REALTIME_INODE macro in fs/xfs/xfs_linux.h in the Linux kernel before 4.13.2 does not verify that a filesystem has a realtime device, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via vectors related to setting an RHINHERIT flag on a directory.
CVE-2017-14341	ImageMagick 7.0.6-6 has a large loop vulnerability in ReadWPGImage in coders/wpg.c, causing CPU exhaustion via a crafted wpg image file.
CVE-2017-14342	ImageMagick 7.0.6-6 has a memory exhaustion vulnerability in ReadWPGImage in coders/wpg.c via a crafted wpg image file.
CVE-2017-14343	ImageMagick 7.0.6-6 has a memory leak vulnerability in ReadXCFImage in coders/xcf.c via a crafted xcf image file.
CVE-2017-14348	LibRaw before 0.18.4 has a heap-based Buffer Overflow in the processCanonCameraInfo function via a crafted file.
CVE-2017-14400	In ImageMagick 7.0.7-1 Q16, the PersistPixelCache function in magick/cache.c mishandles the pixel cache nexus, which allows remote attackers to cause a denial of service (NULL pointer dereference in the function GetVirtualPixels in MagickCore/cache.c) via a crafted file.

CVE-2017-14461	A specially crafted email delivered over SMTP and passed on to Dovecot by MTA can trigger an out of bounds read resulting in potential sensitive information disclosure and denial of service. In order to trigger this vulnerability, an attacker needs to send a specially crafted email message to the server.
CVE-2017-14482	GNU Emacs before 25.3 allows remote attackers to execute arbitrary code via email with crafted "Content-Type: text/enriched" data containing an x-display XML element that specifies execution of shell commands, related to an unsafe text/enriched extension in lisp/textmodes/enriched.el, and unsafe Gnus support for enriched and richtext inline MIME objects in lisp/gnus/mm-view.el. In particular, an Emacs user can be instantly compromised by reading a crafted email message (or Usenet news article).
CVE-2017-14489	The iscsi_if_rx function in drivers/scsi/scsi_transport_iscsi.c in the Linux kernel through 4.13.2 allows local users to cause a denial of service (panic) by leveraging incorrect length validation.
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-2017-14501	An out-of-bounds read flaw exists in parse_file_info in archive_read_support_format_iso9660.c in libarchive 3.3.2 when extracting a

	specially crafted iso9660 iso file, related to archive_read_format_iso9660_read_header.
CVE-2017-14502	read_header in archive_read_support_format_rar.c in libarchive 3.3.2 suffers from an off-by-one error for UTF-16 names in RAR archives, leading to an out-of-bounds read in archive_read_format_rar_read_header.
CVE-2017-14503	libarchive 3.3.2 suffers from an out-of-bounds read within lha_read_data_none() in archive_read_support_format_lha.c when extracting a specially crafted lha archive, related to lha_crc16.
CVE-2017-14505	DrawGetStrokeDashArray in wand/drawing-wand.c in ImageMagick 7.0.7-1 mishandles certain NULL arrays, which allows attackers to perform Denial of Service (NULL pointer dereference and application crash in AcquireQuantumMemory within MagickCore/memory.c) by providing a crafted Image File as input.
CVE-2017-14517	In Poppler 0.59.0, a NULL Pointer Dereference exists in the XRef::parseEntry() function in XRef.cc via a crafted PDF document.
CVE-2017-14518	In Poppler 0.59.0, a floating point exception exists in the isImageInterpolationRequired() function in Splash.cc via a crafted PDF document.
CVE-2017-14519	In Poppler 0.59.0, memory corruption occurs in a call to Object::streamGetChar in Object.h after a repeating series of Gfx::display, Gfx::go, Gfx::execOp, Gfx::opShowText, and Gfx::doShowText calls (aka a Gfx.cc infinite loop).
CVE-2017-14520	In Poppler 0.59.0, a floating point exception occurs in Splash::scaleImageYuXd() in Splash.cc, which may lead to a potential attack when handling malicious PDF files.
CVE-2017-14531	ImageMagick 7.0.7-0 has a memory exhaustion issue in ReadSUNImage in coders/sun.c.
CVE-2017-14532	ImageMagick 7.0.7-0 has a NULL Pointer Dereference in TIFFIgnoreTags in coders/tiff.c.
CVE-2017-14533	ImageMagick 7.0.6-6 has a memory leak in ReadMATImage in coders/mat.c.
CVE-2017-14607	In ImageMagick 7.0.7-4 Q16, an out of bounds read flaw related to ReadTIFFImage has been reported in coders/tiff.c. An attacker could possibly exploit this flaw to disclose potentially sensitive memory or cause an application crash.
CVE-2017-14608	In LibRaw through 0.18.4, an out of bounds read flaw related to kodak_65000_load_raw has been reported in dcraw/dcraw.c and internal/dcraw_common.cpp. An attacker could possibly exploit this flaw to disclose potentially sensitive memory or cause an application crash.

CVE-2017-14617	In Poppler 0.59.0, a floating point exception occurs in the ImageStream class in Stream.cc, which may lead to a potential attack when handling malicious PDF files.
CVE-2017-14624	ImageMagick 7.0.7-0 Q16 has a NULL Pointer Dereference vulnerability in the function PostscriptDelegateMessage in coders/ps.c.
CVE-2017-14625	ImageMagick 7.0.7-0 Q16 has a NULL Pointer Dereference vulnerability in the function sixel_output_create in coders/sixel.c.
CVE-2017-14626	ImageMagick 7.0.7-0 Q16 has a NULL Pointer Dereference vulnerability in the function sixel_decode in coders/sixel.c.
CVE-2017-14632	Xiph.Org libvorbis 1.3.5 allows Remote Code Execution upon freeing uninitialized memory in the function vorbis_analysis_headerout() in info.c when vi->channels<=0, a similar issue to Mozilla bug 550184.
CVE-2017-14633	In Xiph.Org libvorbis 1.3.5, an out-of-bounds array read vulnerability exists in the function mapping0_forward() in mapping0.c, which may lead to DoS when operating on a crafted audio file with vorbis_analysis().
CVE-2017-14682	GetNextToken in MagickCore/token.c in ImageMagick 7.0.6 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted SVG document, a different vulnerability than CVE-2017-10928.
CVE-2017-14684	In ImageMagick 7.0.7-4 Q16, a memory leak vulnerability was found in the function ReadVIPSImage in coders/vips.c, which allows attackers to cause a denial of service (memory consumption in ResizeMagickMemory in MagickCore/memory.c) via a crafted file.
CVE-2017-14739	The AcquireResampleFilterThreadSet function in magick/resample-private.h in ImageMagick 7.0.7-4 mishandles failed memory allocation, which allows remote attackers to cause a denial of service (NULL Pointer Dereference in DistortImage in MagickCore/distort.c, and application crash) via unspecified vectors.
CVE-2017-14741	The ReadCAPTIONImage function in coders/caption.c in ImageMagick 7.0.7-3 allows remote attackers to cause a denial of service (infinite loop) via a crafted font file.
CVE-2017-14746	Use-after-free vulnerability in Samba 4.x before 4.7.3 allows remote attackers to execute arbitrary code via a crafted SMB1 request.
CVE-2017-14859	An Invalid memory address dereference was discovered in Exiv2::StringValueBase::read in value.cpp in Exiv2 0.26. The vulnerability causes a segmentation

	fault and application crash, which leads to denial of service.
CVE-2017-14862	An Invalid memory address dereference was discovered in Exiv2::DataValue::read in value.cpp in Exiv2 0.26. The vulnerability causes a segmentation fault and application crash, which leads to denial of service.
CVE-2017-14864	An Invalid memory address dereference was discovered in Exiv2::getULong in types.cpp in Exiv2 0.26. The vulnerability causes a segmentation fault and application crash, which leads to denial of service.
CVE-2017-14867	Git before 2.10.5, 2.11.x before 2.11.4, 2.12.x before 2.12.5, 2.13.x before 2.13.6, and 2.14.x before 2.14.2 uses unsafe Perl scripts to support subcommands such as cvsserver, which allows attackers to execute arbitrary OS commands via shell metacharacters in a module name. The vulnerable code is reachable via git-shell even without CVS support.
CVE-2017-14926	In Poppler 0.59.0, a NULL Pointer Dereference exists in AnnotRichMedia::Content::Content in Annot.cc via a crafted PDF document.
CVE-2017-14928	In Poppler 0.59.0, a NULL Pointer Dereference exists in AnnotRichMedia::Configuration::Configuration in Annot.cc via a crafted PDF document.
CVE-2017-14929	In Poppler 0.59.0, memory corruption occurs in a call to Object::dictLookup() in Object.h after a repeating series of Gfx::display, Gfx::go, Gfx::execOp, Gfx::opFill, Gfx::doPatternFill, Gfx::doTilingPatternFill and Gfx::drawForm calls (aka a Gfx.cc infinite loop), a different vulnerability than CVE-2017-14519.
CVE-2017-14952	Double free in i18n/zonemeta.cpp in International Components for Unicode (ICU) for C/C++ through 59.1 allows remote attackers to execute arbitrary code via a crafted string, aka a "redundant UVector entry clean up function call" issue.
CVE-2017-14975	The FoFiType1C::convertToType0 function in FoFiType1C.cc in Poppler 0.59.0 has a NULL pointer dereference vulnerability because a data structure is not initialized, which allows an attacker to launch a denial of service attack.
CVE-2017-14976	The FoFiType1C::convertToType0 function in FoFiType1C.cc in Poppler 0.59.0 has a heap-based buffer over-read vulnerability if an out-of-bounds font dictionary index is encountered, which allows an attacker to launch a denial of service attack.
CVE-2017-14977	The FoFiTrueType::getCFFBlock function in FoFiTrueType.cc in Poppler 0.59.0 has a NULL pointer dereference vulnerability due to lack of validation of

	a table pointer, which allows an attacker to launch a denial of service attack.
CVE-2017-14989	A use-after-free in RenderFreetype in MagickCore/annotate.c in ImageMagick 7.0.7-4 Q16 allows attackers to crash the application via a crafted font file, because the FT_Done_Glyph function (from FreeType 2) is called at an incorrect place in the ImageMagick code.
CVE-2017-14991	The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel before 4.13.4 allows local users to obtain sensitive information from uninitialized kernel heap-memory locations via an SG_GET_REQUEST_TABLE ioctl call for /dev/sg0.
CVE-2017-15015	ImageMagick 7.0.7-0 Q16 has a NULL pointer dereference vulnerability in PDFDelegateMessage in coders/pdf.c.
CVE-2017-15016	ImageMagick 7.0.7-0 Q16 has a NULL pointer dereference vulnerability in ReadEnhMetaFile in coders/emf.c.
CVE-2017-15017	ImageMagick 7.0.7-0 Q16 has a NULL pointer dereference vulnerability in ReadOneMNGImage in coders/png.c.
CVE-2017-15032	ImageMagick version 7.0.7-2 contains a memory leak in ReadYCBCRImage in coders/ycbcr.c.
CVE-2017-15033	ImageMagick version 7.0.7-2 contains a memory leak in ReadYUVImage in coders/yuv.c.
CVE-2017-15038	Race condition in the v9fs_xattrwalk function in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allows local guest OS users to obtain sensitive information from host heap memory via vectors related to reading extended attributes.
CVE-2017-15098	Invalid json_populate_recordset or jsonb_populate_recordset function calls in PostgreSQL 10.x before 10.1, 9.6.x before 9.6.6, 9.5.x before 9.5.10, 9.4.x before 9.4.15, and 9.3.x before 9.3.20 can crash the server or disclose a few bytes of server memory.
CVE-2017-15099	INSERT ... ON CONFLICT DO UPDATE commands in PostgreSQL 10.x before 10.1, 9.6.x before 9.6.6, and 9.5.x before 9.5.10 disclose table contents that the invoker lacks privilege to read. These exploits affect only tables where the attacker lacks full read access but has both INSERT and UPDATE privileges. Exploits bypass row level security policies and lack of SELECT privilege.
CVE-2017-15105	A flaw was found in the way unbound before 1.6.8 validated wildcard-synthesized NSEC records. An improperly validated wildcard NSEC record could be used to prove the non-existence (NXDOMAIN answer)

	of an existing wildcard record, or trick unbound into accepting a NODATA proof.
CVE-2017-15115	The sctp_do_peeloff function in net/sctp/socket.c in the Linux kernel before 4.14 does not check whether the intended netns is used in a peel-off action, which allows local users to cause a denial of service (use-after-free and system crash) or possibly have unspecified other impact via crafted system calls.
CVE-2017-15119	The Network Block Device (NBD) server in Quick Emulator (QEMU) before 2.11 is vulnerable to a denial of service issue. It could occur if a client sent large option requests, making the server waste CPU time on reading up to 4GB per request. A client could use this flaw to keep the NBD server from serving other requests, resulting in DoS.
CVE-2017-15129	A use-after-free vulnerability was found in network namespaces code affecting the Linux kernel before 4.14.11. The function get_net_ns_by_id() in net/core/net_namespace.c does not check for the net::count value after it has found a peer network in netns_ids idr, which could lead to double free and memory corruption. This vulnerability could allow an unprivileged local user to induce kernel memory corruption on the system, leading to a crash. Due to the nature of the flaw, privilege escalation cannot be fully ruled out, although it is thought to be unlikely.
CVE-2017-15130	A denial of service flaw was found in dovecot before 2.2.34. An attacker able to generate random SNI server names could exploit TLS SNI configuration lookups, leading to excessive memory usage and the process to restart.
CVE-2017-15132	A flaw was found in dovecot 2.0 up to 2.2.33 and 2.3.0. An abort of SASL authentication results in a memory leak in dovecot's auth client used by login processes. The leak has impact in high performance configuration where same login processes are reused and can cause the process to crash due to memory exhaustion.
CVE-2017-15217	ImageMagick 7.0.7-2 has a memory leak in ReadSGIImage in coders/sgi.c.
CVE-2017-15218	ImageMagick 7.0.7-2 has a memory leak in ReadOneJNGImage in coders/png.c.
CVE-2017-15227	Irssi before 1.0.5, while waiting for the channel synchronisation, may incorrectly fail to remove destroyed channels from the query list, resulting in use-after-free conditions when updating the state later on.
CVE-2017-15228	Irssi before 1.0.5, when installing themes with unterminated colour formatting sequences, may access data beyond the end of the string.

CVE-2017-15232	libjpeg-turbo 1.5.2 has a NULL Pointer Dereference in jdpostct.c and jquant1.c via a crafted JPEG file.
CVE-2017-15265	Race condition in the ALSA subsystem in the Linux kernel before 4.13.8 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted /dev/snd/seq ioctl calls, related to sound/core/seq/seq_clientmgr.c and sound/core/seq/seq_ports.c.
CVE-2017-15275	Samba before 4.7.3 might allow remote attackers to obtain sensitive information by leveraging failure of the server to clear allocated heap memory.
CVE-2017-15277	ReadGIFImage in coders/gif.c in ImageMagick 7.0.6-1 and GraphicsMagick 1.3.26 leaves the palette uninitialized when processing a GIF file that has neither a global nor local palette. If the affected product is used as a library loaded into a process that operates on interesting data, this data sometimes can be leaked via the uninitialized palette.
CVE-2017-15281	ReadPSDImage in coders/psd.c in ImageMagick 7.0.7-6 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted file, related to "Conditional jump or move depends on uninitialised value(s)."
CVE-2017-15289	The mode4and5 write functions in hw/display/cirrus_vga.c in Qemu allow local OS guest privileged users to cause a denial of service (out-of-bounds write access and Qemu process crash) via vectors related to dst calculation.
CVE-2017-15298	Git through 2.14.2 mishandles layers of tree objects, which allows remote attackers to cause a denial of service (memory consumption) via a crafted repository, aka a Git bomb. This can also have an impact of disk consumption; however, an affected process typically would not survive its attempt to build the data structure in memory before writing to disk.
CVE-2017-15299	The KEYS subsystem in the Linux kernel through 4.13.7 mishandles use of add_key for a key that already exists but is uninstantiated, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted system call.
CVE-2017-15306	The kvm_vm_ioctl_check_extension function in arch/powerpc/kvm/powerpc.c in the Linux kernel before 4.13.11 allows local users to cause a denial of service (NULL pointer dereference and system crash) via a KVM_CHECK_EXTENSION KVM_CAP_PPC_HTM ioctl call to /dev/kvm.
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	Unsafe navigation in Chromecast in Google Chrome prior to 63.0.3239.84 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2017-15537	The x86/fpu (Floating Point Unit) subsystem in the Linux kernel before 4.13.5, when a processor supports the xsave feature but not the xsaves feature, does not correctly handle attempts to set reserved bits in the xstate header via the ptrace() or rt_sigreturn() system

	call, allowing local users to read the FPU registers of other processes on the system, related to arch/x86/kernel/fpu/regset.c and arch/x86/kernel/fpu/signal.c.
CVE-2017-15565	In Poppler 0.59.0, a NULL Pointer Dereference exists in the GfxImageColorMap::getGrayLine() function in GfxState.cc via a crafted PDF document.
CVE-2017-15649	net/packet/af_packet.c in the Linux kernel before 4.13.6 allows local users to gain privileges via crafted system calls that trigger mishandling of packet_fanout data structures, because of a race condition (involving fanout_add and packet_do_bind) that leads to a use-after-free, a different vulnerability than CVE-2017-6346.
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-2017-15706	As part of the fix for bug 61201, the documentation for Apache Tomcat 9.0.0.M22 to 9.0.1, 8.5.16 to 8.5.23, 8.0.45 to 8.0.47 and 7.0.79 to 7.0.82 included an updated description of the search algorithm used by the CGI Servlet to identify which script to execute. The update was not correct. As a result, some scripts may have failed to execute as expected and other scripts may have been executed unexpectedly. Note that the behaviour of the CGI servlet has remained unchanged in this regard. It is only the documentation of the behaviour that was wrong and has been corrected.
CVE-2017-15710	In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language

	header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.
CVE-2017-15715	In Apache httpd 2.4.0 to 2.4.29, the expression specified in <FilesMatch> could match '$' to a newline character in a malicious filename, rather than matching only the end of the filename. This could be exploited in environments where uploads of some files are are externally blocked, but only by matching the trailing portion of the filename.
CVE-2017-15721	In Irssi before 1.0.5, certain incorrectly formatted DCC CTCP messages could cause a NULL pointer dereference. This is a separate, but similar, issue relative to CVE-2017-9468.
CVE-2017-15722	In certain cases, Irssi before 1.0.5 may fail to verify that a Safe channel ID is long enough, causing reads beyond the end of the string.
CVE-2017-15723	In Irssi before 1.0.5, overlong nicks or targets may result in a NULL pointer dereference while splitting the message.
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-2017-15908	In systemd 223 through 235, a remote DNS server can respond with a custom crafted DNS NSEC resource record to trigger an infinite loop in the dns_packet_read_type_window() function of the 'systemd-resolved' service and cause a DoS of the affected service.
CVE-2017-15951	The KEYS subsystem in the Linux kernel before 4.13.10 does not correctly synchronize the actions of updating versus finding a key in the "negative" state to avoid a race condition, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls.
CVE-2017-16227	The aspath_put function in bgpd/bgp_aspath.c in Quagga before 1.2.2 allows remote attackers to cause

	a denial of service (session drop) via BGP UPDATE messages, because AS_PATH size calculation for long paths counts certain bytes twice and consequently constructs an invalid message.
CVE-2017-16525	The usb_serial_console_disconnect function in drivers/usb/serial/console.c in the Linux kernel before 4.13.8 allows local users to cause a denial of service (use-after-free and system crash) or possibly have unspecified other impact via a crafted USB device, related to disconnection and failed setup.
CVE-2017-16526	drivers/uwb/uwbd.c in the Linux kernel before 4.13.6 allows local users to cause a denial of service (general protection fault and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16527	sound/usb/mixer.c in the Linux kernel before 4.13.8 allows local users to cause a denial of service (snd_usb_mixer_interrupt use-after-free and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16528	sound/core/seq_device.c in the Linux kernel before 4.13.4 allows local users to cause a denial of service (snd_rawmidi_dev_seq_free use-after-free and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16529	The snd_usb_create_streams function in sound/usb/card.c in the Linux kernel before 4.13.6 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16530	The uas driver in the Linux kernel before 4.13.6 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device, related to drivers/usb/storage/uas-detect.h and drivers/usb/storage/uas.c.
CVE-2017-16531	drivers/usb/core/config.c in the Linux kernel before 4.13.6 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device, related to the USB_DT_INTERFACE_ASSOCIATION descriptor.
CVE-2017-16532	The get_endpoints function in drivers/usb/misc/usbtest.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16533	The usbhid_parse function in drivers/hid/usbhid/hid-core.c in the Linux kernel before 4.13.8 allows local users to cause a denial of service (out-of-bounds read

	and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16534	The cdc_parse_cdc_header function in drivers/usb/core/message.c in the Linux kernel before 4.13.6 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16535	The usb_get_bos_descriptor function in drivers/usb/core/config.c in the Linux kernel before 4.13.10 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16536	The cx231xx_usb_probe function in drivers/media/usb/cx231xx/cx231xx-cards.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16537	The imon_probe function in drivers/media/rc/imon.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16538	drivers/media/usb/dvb-usb-v2/lmedm04.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (general protection fault and system crash) or possibly have unspecified other impact via a crafted USB device, related to a missing warm-start check and incorrect attach timing (dm04_lme2510_frontend_attach versus dm04_lme2510_tuner).
CVE-2017-16546	The ReadWPGImage function in coders/wpg.c in ImageMagick 7.0.7-9 does not properly validate the colormap index in a WPG palette, which allows remote attackers to cause a denial of service (use of uninitialized data or invalid memory allocation) or possibly have unspecified other impact via a malformed WPG file.
CVE-2017-16548	The receive_xattr function in xattrs.c in rsync 3.1.2 and 3.1.3-development does not check for a trailing '\0' character in an xattr name, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact by sending crafted data to the daemon.
CVE-2017-16611	In libXfont before 1.5.4 and libXfont2 before 2.0.3, a local attacker can open (but not read) files on the system as root, triggering tape rewinds, watchdogs, or similar mechanisms that can be triggered by opening files.

CVE-2017-16612	libXcursor before 1.1.15 has various integer overflows that could lead to heap buffer overflows when processing malicious cursors, e.g., with programs like GIMP. It is also possible that an attack vector exists against the related code in cursor/xcursor.c in Wayland through 1.14.0.
CVE-2017-16643	The parse_hid_report_descriptor function in drivers/input/tablet/gtco.c in the Linux kernel before 4.13.11 allows local users to cause a denial of service (out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16645	The ims_pcu_get_cdc_union_desc function in drivers/input/misc/ims-pcu.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (ims_pcu_parse_cdc_data out-of-bounds read and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16646	drivers/media/usb/dvb-usb/dib0700_devices.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (BUG and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16647	drivers/net/usb/asix_devices.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16649	The usbnet_generic_cdc_bind function in drivers/net/usb/cdc_ether.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (divide-by-zero error and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16650	The qmi_wwan_bind function in drivers/net/usb/qmi_wwan.c in the Linux kernel through 4.13.11 allows local users to cause a denial of service (divide-by-zero error and system crash) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-16844	Heap-based buffer overflow in the loadbuf function in formisc.c in formail in procmail 3.22 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted e-mail message because of a hardcoded realloc size, a different vulnerability than CVE-2014-3618.
CVE-2017-16845	hw/input/ps2.c in Qemu does not validate 'rptr' and 'count' values during guest migration, leading to out-of-bounds access.
CVE-2017-16909	An error related to the "LibRaw::panasonic_load_raw()" function (dcraw_common.cpp) in LibRaw versions prior to 0.18.6 can be exploited to cause a heap-based

	buffer overflow and subsequently cause a crash via a specially crafted TIFF image.
CVE-2017-16910	An error within the "LibRaw::xtrans_interpolate()" function (internal/dcraw_common.cpp) in LibRaw versions prior to 0.18.6 can be exploited to cause an invalid read memory access and subsequently a Denial of Service condition.
CVE-2017-16911	The vhci_hcd driver in the Linux Kernel before version 4.14.8 and 4.4.114 allows allows local attackers to disclose kernel memory addresses. Successful exploitation requires that a USB device is attached over IP.
CVE-2017-16912	The "get_pipe()" function (drivers/usb/usbip/stub_rx.c) in the Linux Kernel before version 4.14.8, 4.9.71, and 4.4.114 allows attackers to cause a denial of service (out-of-bounds read) via a specially crafted USB over IP packet.
CVE-2017-16913	The "stub_recv_cmd_submit()" function (drivers/usb/usbip/stub_rx.c) in the Linux Kernel before version 4.14.8, 4.9.71, and 4.4.114 when handling CMD_SUBMIT packets allows attackers to cause a denial of service (arbitrary memory allocation) via a specially crafted USB over IP packet.
CVE-2017-16914	The "stub_send_ret_submit()" function (drivers/usb/usbip/stub_tx.c) in the Linux Kernel before version 4.14.8, 4.9.71, 4.1.49, and 4.4.107 allows attackers to cause a denial of service (NULL pointer dereference) via a specially crafted USB over IP packet.
CVE-2017-16932	parser.c in libxml2 before 2.9.5 does not prevent infinite recursion in parameter entities.
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-2017-16994	The walk_hugetlb_range function in mm/pagewalk.c in the Linux kernel before 4.14.2 mishandles holes in hugetlb ranges, which allows local users to obtain sensitive information from uninitialized kernel memory via crafted use of the mincore() system call.
CVE-2017-16995	The check_alu_op function in kernel/bpf/verifier.c in the Linux kernel through 4.14.8 allows local users to cause a denial of service (memory corruption) or possibly have unspecified other impact by leveraging incorrect sign extension.
CVE-2017-16997	elf/dl-load.c in the GNU C Library (aka glibc or libc6) 2.19 through 2.26 mishandles RPATH and RUNPATH containing $ORIGIN for a privileged (setuid

	or AT_SECURE) program, which allows local users to gain privileges via a Trojan horse library in the current working directory, related to the fillin_rpath and decompose_rpath functions. This is associated with misinterpretion of an empty RPATH/RUNPATH token as the "./" directory. NOTE: this configuration of RPATH/RUNPATH for a privileged program is apparently very uncommon; most likely, no such program is shipped with any common Linux distribution.
CVE-2017-17095	tools/pal2rgb.c in pal2rgb in LibTIFF 4.0.9 allows remote attackers to cause a denial of service (TIFFSetupStrips heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted TIFF file.
CVE-2017-17381	The Virtio Vring implementation in QEMU allows local OS guest users to cause a denial of service (divide-by-zero error and QEMU process crash) by unsetting vring alignment while updating Virtio rings.
CVE-2017-17405	Ruby before 2.4.3 allows Net::FTP command injection. Net::FTP#get, getbinaryfile, gettextfile, put, putbinaryfile, and puttextfile use Kernel#open to open a local file. If the localfile argument starts with the "|" pipe character, the command following the pipe character is executed. The default value of localfile is File.basename(remotefile), so malicious FTP servers could cause arbitrary command execution.
CVE-2017-17426	The malloc function in the GNU C Library (aka glibc or libc6) 2.26 could return a memory block that is too small if an attempt is made to allocate an object whose size is close to SIZE_MAX, potentially leading to a subsequent heap overflow. This occurs because the per-thread cache (aka tcache) feature enables a code path that lacks an integer overflow check.
CVE-2017-17433	The recv_files function in receiver.c in the daemon in rsync 3.1.2, and 3.1.3-development before 2017-12-03, proceeds with certain file metadata updates before checking for a filename in the daemon_filter_list data structure, which allows remote attackers to bypass intended access restrictions.
CVE-2017-17434	The daemon in rsync 3.1.2, and 3.1.3-development before 2017-12-03, does not check for fnamecmp filenames in the daemon_filter_list data structure (in the recv_files function in receiver.c) and also does not apply the sanitize_paths protection mechanism to pathnames found in "xname follows" strings (in the read_ndx_and_attrs function in rsync.c), which allows remote attackers to bypass intended access restrictions.
CVE-2017-17448	net/netfilter/nfnetlink_cthelper.c in the Linux kernel through 4.14.4 does not require the CAP_NET_ADMIN capability for new, get, and del operations, which allows

	local users to bypass intended access restrictions because the nfnl_cthelper_list data structure is shared across all net namespaces.
CVE-2017-17449	The __netlink_deliver_tap_skb function in net/netlink/af_netlink.c in the Linux kernel through 4.14.4, when CONFIG_NLMON is enabled, does not restrict observations of Netlink messages to a single net namespace, which allows local users to obtain sensitive information by leveraging the CAP_NET_ADMIN capability to sniff an nlmon interface for all Netlink activity on the system.
CVE-2017-17450	net/netfilter/xt_osf.c in the Linux kernel through 4.14.4 does not require the CAP_NET_ADMIN capability for add_callback and remove_callback operations, which allows local users to bypass intended access restrictions because the xt_osf_fingers data structure is shared across all net namespaces.
CVE-2017-17485	FasterXML jackson-databind through 2.8.10 and 2.9.x through 2.9.3 allows unauthenticated remote code execution because of an incomplete fix for the CVE-2017-7525 deserialization flaw. This is exploitable by sending maliciously crafted JSON input to the readValue method of the ObjectMapper, bypassing a blacklist that is ineffective if the Spring libraries are available in the classpath.
CVE-2017-17499	ImageMagick before 6.9.9-24 and 7.x before 7.0.7-12 has a use-after-free in Magick::Image::read in Magick++/lib/Image.cpp.
CVE-2017-17504	ImageMagick before 7.0.7-12 has a coders/png.c Magick_png_read_raw_profile heap-based buffer over-read via a crafted file, related to ReadOneMNGImage.
CVE-2017-17512	sensible-browser in sensible-utils before 0.0.11 does not validate strings before launching the program specified by the BROWSER environment variable, which allows remote attackers to conduct argument-injection attacks via a crafted URL, as demonstrated by a --proxy-pac-file argument.
CVE-2017-17558	The usb_destroy_configuration function in drivers/usb/core/config.c in the USB core subsystem in the Linux kernel through 4.14.5 does not consider the maximum number of configurations and interfaces before attempting to release resources, which allows local users to cause a denial of service (out-of-bounds write access) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-17669	There is a heap-based buffer over-read in the Exiv2::Internal::PngChunk::keyTXTChunk function of pngchunk_int.cpp in Exiv2 0.26. A crafted PNG file will lead to a remote denial of service attack.

CVE-2017-17680	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadXPMImage in coders/xpm.c, which allows attackers to cause a denial of service via a crafted xpm image file.
CVE-2017-17681	In ImageMagick 7.0.7-12 Q16, an infinite loop vulnerability was found in the function ReadPSDChannelZip in coders/psd.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted psd image file.
CVE-2017-17682	In ImageMagick 7.0.7-12 Q16, a large loop vulnerability was found in the function ExtractPostscript in coders/wpg.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted wpg image file that triggers a ReadWPGImage call.
CVE-2017-17712	The raw_sendmsg() function in net/ipv4/raw.c in the Linux kernel through 4.14.6 has a race condition in inet->hdrincl that leads to uninitialized stack pointer usage; this allows a local user to execute code and gain privileges.
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-2017-17805	The Salsa20 encryption algorithm in the Linux kernel before 4.14.8 does not correctly handle zero-length inputs, allowing a local attacker able to use the AF_ALG-based skcipher interface (CONFIG_CRYPTO_USER_API_SKCIPHER) to cause a denial of service (uninitialized-memory free and kernel crash) or have unspecified other impact by executing a crafted sequence of system calls that use the blkcipher_walk API. Both the generic implementation (crypto/salsa20_generic.c) and x86 implementation (arch/x86/crypto/salsa20_glue.c) of Salsa20 were vulnerable.
CVE-2017-17806	The HMAC implementation (crypto/hmac.c) in the Linux kernel before 4.14.8 does not

	validate that the underlying cryptographic hash algorithm is unkeyed, allowing a local attacker able to use the AF_ALG-based hash interface (CONFIG_CRYPTO_USER_API_HASH) and the SHA-3 hash algorithm (CONFIG_CRYPTO_SHA3) to cause a kernel stack buffer overflow by executing a crafted sequence of system calls that encounter a missing SHA-3 initialization.
CVE-2017-17807	The KEYS subsystem in the Linux kernel before 4.14.6 omitted an access-control check when adding a key to the current task's "default request-key keyring" via the request_key() system call, allowing a local user to use a sequence of crafted system calls to add keys to a keyring with only Search permission (not Write permission) to that keyring, related to construct_get_dest_keyring() in security/keys/request_key.c.
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-2017-17862	kernel/bpf/verifier.c in the Linux kernel through 4.14.8 ignores unreachable code, even though it would still be processed by JIT compilers. This behavior, also considered an improper branch-pruning logic issue, could possibly be used by local users for denial of service.
CVE-2017-17863	kernel/bpf/verifier.c in the Linux kernel 4.9.x through 4.9.71 does not check the relationship between pointer values and the BPF stack, which allows local users to cause a denial of service (integer overflow or invalid memory access) or possibly have unspecified other impact.
CVE-2017-17864	kernel/bpf/verifier.c in the Linux kernel through 4.14.8 mishandles states_equal comparisons between the pointer data type and the UNKNOWN_VALUE data type, which allows local users to obtain potentially sensitive address information, aka a "pointer leak."
CVE-2017-17879	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-21, there is a heap-based buffer over-read in ReadOneMNGImage in coders/png.c, related to length calculation and caused by an off-by-one error.
CVE-2017-17881	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allows attackers to cause a denial of service via a crafted MAT image file.
CVE-2017-17882	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadXPMImage in coders/xpm.c, which allows attackers to cause a denial of service via a crafted XPM image file.

CVE-2017-17884	In ImageMagick 7.0.7-16 Q16, a memory leak vulnerability was found in the function WriteOnePNGImage in coders/png.c, which allows attackers to cause a denial of service via a crafted PNG image file.
CVE-2017-17885	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadPICTImage in coders/pict.c, which allows attackers to cause a denial of service via a crafted PICT image file.
CVE-2017-17886	In ImageMagick 7.0.7-12 Q16, a memory leak vulnerability was found in the function ReadPSDChannelZip in coders/psd.c, which allows attackers to cause a denial of service via a crafted psd image file.
CVE-2017-17887	In ImageMagick 7.0.7-16 Q16, a memory leak vulnerability was found in the function GetImagePixelCache in magick/cache.c, which allows attackers to cause a denial of service via a crafted MNG image file that is processed by ReadOneMNGImage.
CVE-2017-17914	In ImageMagick 7.0.7-16 Q16, a vulnerability was found in the function ReadOnePNGImage in coders/png.c, which allows attackers to cause a denial of service (ReadOneMNGImage large loop) via a crafted mng image file.
CVE-2017-17934	ImageMagick 7.0.7-17 Q16 x86_64 has memory leaks in coders/msl.c, related to MSLPopImage and ProcessMSLScript, and associated with mishandling of MSLPushImage calls.
CVE-2017-17975	Use-after-free in the usbtv_probe function in drivers/media/usb/usbtv/usbtv-core.c in the Linux kernel through 4.14.10 allows attackers to cause a denial of service (system crash) or possibly have unspecified other impact by triggering failure of audio registration, because a kfree of the usbtv data structure occurs during a usbtv_video_free call, but the usbtv_video_fail label's code attempts to both access and free this data structure.
CVE-2017-18008	In ImageMagick 7.0.7-17 Q16, there is a Memory Leak in ReadPWPImage in coders/pwp.c.
CVE-2017-18013	In LibTIFF 4.0.9, there is a Null-Pointer Dereference in the tif_print.c TIFFPrintDirectory function, as demonstrated by a tiffinfo crash.
CVE-2017-18022	In ImageMagick 7.0.7-12 Q16, there are memory leaks in MontageImageCommand in MagickWand/montage.c.
CVE-2017-18027	In ImageMagick 7.0.7-1 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allow remote attackers to cause a denial of service via a crafted file.

CVE-2017-18028	In ImageMagick 7.0.7-1 Q16, a memory exhaustion vulnerability was found in the function ReadTIFFImage in coders/tiff.c, which allow remote attackers to cause a denial of service via a crafted file.
CVE-2017-18029	In ImageMagick 7.0.6-10 Q16, a memory leak vulnerability was found in the function ReadMATImage in coders/mat.c, which allow remote attackers to cause a denial of service via a crafted file.
CVE-2017-18043	Integer overflow in the macro ROUND_UP (n, d) in Quick Emulator (Qemu) allows a user to cause a denial of service (Qemu process crash).
CVE-2017-18075	crypto/pcrypt.c in the Linux kernel before 4.14.13 mishandles freeing instances, allowing a local user able to access the AF_ALG-based AEAD interface (CONFIG_CRYPTO_USER_API_AEAD) and pcrypt (CONFIG_CRYPTO_PCRYPT) to cause a denial of service (kfree of an incorrect pointer) or possibly have unspecified other impact by executing a crafted sequence of system calls.
CVE-2017-18183	An issue was discovered in QPDF before 7.0.0. There is an infinite loop in the QPDFWriter::enqueueObject() function in libqpdf/QPDFWriter.cc.
CVE-2017-18184	An issue was discovered in QPDF before 7.0.0. There is a stack-based out-of-bounds read in the function iterate_rc4 in QPDF_encryption.cc.
CVE-2017-18185	An issue was discovered in QPDF before 7.0.0. There is a large heap-based out-of-bounds read in the PI_Buffer::write function in PI_Buffer.cc. It is caused by an integer overflow in the PNG filter.
CVE-2017-18186	An issue was discovered in QPDF before 7.0.0. There is an infinite loop due to looping xref tables in QPDF.cc.
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-2017-18193	fs/f2fs/extent_cache.c in the Linux kernel before 4.13 mishandles extent trees, which allows local users to cause a denial of service (BUG) via an application with multiple threads.
CVE-2017-18203	The dm_get_from_kobject function in drivers/md/dm.c in the Linux kernel before 4.14.3 allow local users to cause a denial of service (BUG) by leveraging a race condition with __dm_destroy during creation and removal of DM devices.

CVE-2017-18204	The ocfs2_setattr function in fs/ocfs2/file.c in the Linux kernel before 4.14.2 allows local users to cause a denial of service (deadlock) via DIO requests.
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-2017-18208	The madvise_willneed function in mm/madvise.c in the Linux kernel before 4.14.4 allows local users to cause a denial of service (infinite loop) by triggering use of MADVISE_WILLNEED for a DAX mapping.
CVE-2017-18209	In the GetOpenCLCachedFilesDirectory function in magick/opencl.c in ImageMagick 7.0.7, a NULL pointer dereference vulnerability occurs because a memory allocation result is not checked, related to GetOpenCLCacheDirectory.
CVE-2017-18211	In ImageMagick 7.0.7, a NULL pointer dereference vulnerability was found in the function saveBinaryCLProgram in magick/opencl.c because a program-lookup result is not checked, related to CacheOpenCLKernel.
CVE-2017-18216	In fs/ocfs2/cluster/nodemanager.c in the Linux kernel before 4.15, local users can cause a denial of service (NULL pointer dereference and BUG) because a required mutex is not used.
CVE-2017-18222	In the Linux kernel before 4.12, Hisilicon Network Subsystem (HNS) does not consider the ETH_SS_PRIV_FLAGS case when retrieving sset_count data, which allows local users to cause a denial of service (buffer overflow and memory corruption) or possibly have unspecified other impact, as demonstrated by incompatibility between hns_get_sset_count and ethtool_get_strings.
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-2017-18255	The perf_cpu_time_max_percent_handler function in kernel/events/core.c in the Linux kernel before 4.11 allows local users to cause a denial of service (integer overflow) or possibly have unspecified other impact via a large value, as demonstrated by an incorrect sample-rate calculation.
CVE-2017-18257	The __get_data_block function in fs/f2fs/data.c in the Linux kernel before 4.11 allows local users to cause a denial of service (integer overflow and loop) via crafted use of the open and fallocate system calls with an FS_IOC_FIEMAP ioctl.
CVE-2017-18258	The xz_head function in xzlib.c in libxml2 before 2.9.6 allows remote attackers to cause a denial of service (memory consumption) via a crafted LZMA file, because the decoder functionality does not restrict memory usage to what is required for a legitimate file.
CVE-2017-18266	The open_envvar function in xdg-open in xdg-utils before 1.1.3 does not validate strings before launching the program specified by the BROWSER environment variable, which might allow remote attackers to conduct argument-injection attacks via a crafted URL, as demonstrated by %s in this environment variable.
CVE-2017-18267	The FoFiType1C::cvtGlyph function in fofi/FoFiType1C.cc in Poppler through 0.64.0 allows remote

	attackers to cause a denial of service (infinite recursion) via a crafted PDF file, as demonstrated by pdftops.
CVE-2017-18271	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-22, an infinite loop vulnerability was found in the function ReadMIFFImage in coders/miff.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted MIFF image file.
CVE-2017-18273	In ImageMagick 7.0.7-16 Q16 x86_64 2017-12-22, an infinite loop vulnerability was found in the function ReadTXTImage in coders/txt.c, which allows attackers to cause a denial of service (CPU exhaustion) via a crafted image file that is mishandled in a GetImageIndexInList call.
CVE-2017-2350	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. tvOS before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.
CVE-2017-2354	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. iCloud before 6.1.1 is affected. iTunes before 12.5.5 is affected. tvOS before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2355	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. iCloud before 6.1.1 is affected. iTunes before 12.5.5 is affected. tvOS before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (uninitialized memory access and application crash) via a crafted web site.
CVE-2017-2356	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. iCloud before 6.1.1 is affected. iTunes before 12.5.5 is affected. tvOS before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2362	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. tvOS before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-2363	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. tvOS before 10.1.1 is affected. watchOS before 3.1.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.
CVE-2017-2364	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.
CVE-2017-2365	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. tvOS before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.
CVE-2017-2366	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. iCloud before 6.1.1 is affected. iTunes before 12.5.5 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2367	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.
CVE-2017-2369	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. tvOS before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2371	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. The issue involves the "WebKit" component, which allows remote attackers to launch popups via a crafted web site.
CVE-2017-2373	An issue was discovered in certain Apple products. iOS before 10.2.1 is affected. Safari before 10.0.3 is affected. tvOS before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-2376	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "Safari" component. It allows remote attackers to spoof the address bar by leveraging text input during the loading of a page.
CVE-2017-2377	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit Web Inspector" component. It allows attackers to cause a denial of service (memory corruption and application crash) by leveraging a window-close action during a debugger-pause state.
CVE-2017-2386	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.
CVE-2017-2392	An issue was discovered in certain Apple products. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted app.
CVE-2017-2394	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2395	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2396	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2405	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit Web Inspector" 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-2017-2415	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. watchOS before 3.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code by leveraging an unspecified "type confusion."
CVE-2017-2419	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass a Content Security Policy protection mechanism via unspecified vectors.
CVE-2017-2433	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2442	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit JavaScript Bindings" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive information via a crafted web site.
CVE-2017-2445	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via crafted frame objects.
CVE-2017-2446	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code via a crafted web site that leverages the mishandling of strict mode functions.
CVE-2017-2447	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive information or cause a denial of service (memory corruption) via a crafted web site.
CVE-2017-2454	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2455	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected.

	tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2457	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2459	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2460	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2464	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2465	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2466	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2468	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service

	(memory corruption and application crash) via a crafted web site.
CVE-2017-2469	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2470	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2471	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. watchOS before 3.2 is affected. The issue involves the "WebKit" component. A use-after-free vulnerability allows remote attackers to execute arbitrary code via a crafted web site.
CVE-2017-2475	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via crafted use of frames on a web site.
CVE-2017-2476	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2481	An issue was discovered in certain Apple products. iOS before 10.3 is affected. Safari before 10.1 is affected. tvOS before 10.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2496	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2510	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is

	affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that improperly interacts with pageshow events.
CVE-2017-2539	An issue was discovered in certain Apple products. iOS before 10.3.2 is affected. Safari before 10.1.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-2583	The load_segment_descriptor implementation in arch/x86/kvm/emulate.c in the Linux kernel before 4.9.5 improperly emulates a "MOV SS, NULL selector" instruction, which allows guest OS users to cause a denial of service (guest OS crash) or gain guest OS privileges via a crafted application.
CVE-2017-2584	arch/x86/kvm/emulate.c in the Linux kernel through 4.9.3 allows local users to obtain sensitive information from kernel memory or cause a denial of service (use-after-free) via a crafted application that leverages instruction emulation for fxrstor, fxsave, sgdt, and sidt.
CVE-2017-2592	python-oslo-middleware before versions 3.8.1, 3.19.1, 3.23.1 is vulnerable to an information disclosure. Software using the CatchError class could include sensitive values in a traceback's error message. System users could exploit this flaw to obtain sensitive information from OpenStack component error logs (for example, keystone tokens).
CVE-2017-2596	The nested_vmx_check_vmptr function in arch/x86/kvm/vmx.c in the Linux kernel through 4.9.8 improperly emulates the VMXON instruction, which allows KVM L1 guest OS users to cause a denial of service (host OS memory consumption) by leveraging the mishandling of page references.
CVE-2017-2615	Quick emulator (QEMU) built with the Cirrus CLGD 54xx VGA emulator support is vulnerable to an out-of-bounds access issue. It could occur while copying VGA data via bitblt copy in backward mode. A privileged user inside a guest could use this flaw to crash the QEMU process resulting in DoS or potentially execute arbitrary code on the host with privileges of QEMU process on the host.
CVE-2017-2616	A race condition was found in util-linux before 2.32.1 in the way su handled the management of child processes. A local authenticated attacker could use this flaw to kill other processes with root privileges under specific conditions.
CVE-2017-2618	A flaw was found in the Linux kernel's handling of clearing SELinux attributes on /proc/pid/attr files before 4.9.10. An empty (null) write to this file can crash the

	system by causing the system to attempt to access unmapped kernel memory.
CVE-2017-2619	Samba before versions 4.6.1, 4.5.7 and 4.4.11 are vulnerable to a malicious client using a symlink race to allow access to areas of the server file system not exported under the share definition.
CVE-2017-2620	Quick emulator (QEMU) before 2.8 built with the Cirrus CLGD 54xx VGA Emulator support is vulnerable to an out-of-bounds access issue. The issue could occur while copying VGA data in cirrus_bitblt_cputovideo. A privileged user inside guest could use this flaw to crash the QEMU process OR potentially execute arbitrary code on host with privileges of the QEMU process.
CVE-2017-2624	It was found that xorg-x11-server before 1.19.0 including uses memcmp() to check the received MIT cookie against a series of valid cookies. If the cookie is correct, it is allowed to attach to the Xorg session. Since most memcmp() implementations return after an invalid byte is seen, this causes a time difference between a valid and invalid byte, which could allow an efficient brute force attack.
CVE-2017-2633	An out-of-bounds memory access issue was found in Quick Emulator (QEMU) before 1.7.2 in the VNC display driver. This flaw could occur while refreshing the VNC display surface area in the 'vnc_refresh_server_surface'. A user inside a guest could use this flaw to crash the QEMU process.
CVE-2017-2636	Race condition in drivers/tty/n_hdlc.c in the Linux kernel through 4.10.1 allows local users to gain privileges or cause a denial of service (double free) by setting the HDLC line discipline.
CVE-2017-2669	Dovecot before version 2.2.29 is vulnerable to a denial of service. When 'dict' passdb and userdb were used for user authentication, the username sent by the IMAP/POP3 client was sent through var_expand() to perform %variable expansion. Sending specially crafted %variable fields could result in excessive memory usage causing the process to crash (and restart), or excessive CPU usage causing all authentications to hang.
CVE-2017-2671	The ping_unhash function in net/ipv4/ping.c in the Linux kernel through 4.10.8 is too late in obtaining a certain lock and consequently cannot ensure that disconnect function calls are safe, which allows local users to cause a denial of service (panic) by leveraging access to the protocol value of IPPROTO_ICMP in a socket system call.
CVE-2017-2820	An exploitable integer overflow vulnerability exists in the JPEG 2000 image parsing functionality of freedesktop.org Poppler 0.53.0. A specially crafted

	PDF file can lead to an integer overflow causing out of bounds memory overwrite on the heap resulting in potential arbitrary code execution. To trigger this vulnerability, a victim must open the malicious PDF in an application using this library.
CVE-2017-2824	An exploitable code execution vulnerability exists in the trapper command functionality of Zabbix Server 2.4.X. A specially crafted set of packets can cause a command injection resulting in remote code execution. An attacker can make requests from an active Zabbix Proxy to trigger this vulnerability.
CVE-2017-2834	An exploitable code execution vulnerability exists in the authentication functionality of FreeRDP 2.0.0-beta1+android11. A specially crafted server response can cause an out-of-bounds write resulting in an exploitable condition. An attacker can compromise the server or use a man in the middle attack to trigger this vulnerability.
CVE-2017-2835	An exploitable code execution vulnerability exists in the RDP receive functionality of FreeRDP 2.0.0-beta1+android11. A specially crafted server response can cause an out-of-bounds write resulting in an exploitable condition. An attacker can compromise the server or use a man in the middle to trigger this vulnerability.
CVE-2017-2836	An exploitable denial of service vulnerability exists within the reading of proprietary server certificates in FreeRDP 2.0.0-beta1+android11. A specially crafted challenge packet can cause the program termination leading to a denial of service condition. An attacker can compromise the server or use man in the middle to trigger this vulnerability.
CVE-2017-2837	An exploitable denial of service vulnerability exists within the handling of security data in FreeRDP 2.0.0-beta1+android11. A specially crafted challenge packet can cause the program termination leading to a denial of service condition. An attacker can compromise the server or use man in the middle to trigger this vulnerability.
CVE-2017-2838	An exploitable denial of service vulnerability exists within the handling of challenge packets in FreeRDP 2.0.0-beta1+android11. A specially crafted challenge packet can cause the program termination leading to a denial of service condition. An attacker can compromise the server or use man in the middle to trigger this vulnerability.
CVE-2017-2839	An exploitable denial of service vulnerability exists within the handling of challenge packets in FreeRDP 2.0.0-beta1+android11. A specially crafted challenge packet can cause the program termination leading to a denial of service condition. An attacker can compromise

	the server or use man in the middle to trigger this vulnerability.
CVE-2017-2862	An exploitable heap overflow vulnerability exists in the gdk_pixbuf__jpeg_image_load_increment functionality of Gdk-Pixbuf 2.36.6. A specially crafted jpeg file can cause a heap overflow resulting in remote code execution. An attacker can send a file or url to trigger this vulnerability.
CVE-2017-2870	An exploitable integer overflow vulnerability exists in the tiff_image_parse functionality of Gdk-Pixbuf 2.36.6 when compiled with Clang. A specially crafted tiff file can cause a heap-overflow resulting in remote code execution. An attacker can send a file or a URL to trigger this vulnerability.
CVE-2017-2885	An exploitable stack based buffer overflow vulnerability exists in the GNOME libsoup 2.58. A specially crafted HTTP request can cause a stack overflow resulting in remote code execution. An attacker can send a special HTTP request to the vulnerable server to trigger this vulnerability.
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-2017-3135	Under some conditions when using both DNS64 and RPZ to rewrite query responses, query processing can

	resume in an inconsistent state leading to either an INSIST assertion failure or an attempt to read through a NULL pointer. Affects BIND 9.8.8, 9.9.3-S1 -> 9.9.9-S7, 9.9.3 -> 9.9.9-P5, 9.9.10b1, 9.10.0 -> 9.10.4-P5, 9.10.5b1, 9.11.0 -> 9.11.0-P2, 9.11.1b1.
CVE-2017-3136	A query with a specific set of characteristics could cause a server using DNS64 to encounter an assertion failure and terminate. An attacker could deliberately construct a query, enabling denial-of-service against a server if it was configured to use the DNS64 feature and other preconditions were met. Affects BIND 9.8.0 -> 9.8.8-P1, 9.9.0 -> 9.9.9-P6, 9.9.10b1->9.9.10rc1, 9.10.0 -> 9.10.4-P6, 9.10.5b1->9.10.5rc1, 9.11.0 -> 9.11.0-P3, 9.11.1b1->9.11.1rc1, 9.9.3-S1 -> 9.9.9-S8.
CVE-2017-3137	Mistaken assumptions about the ordering of records in the answer section of a response containing CNAME or DNAME resource records could lead to a situation in which named would exit with an assertion failure when processing a response in which records occurred in an unusual order. Affects BIND 9.9.9-P6, 9.9.10b1->9.9.10rc1, 9.10.4-P6, 9.10.5b1->9.10.5rc1, 9.11.0-P3, 9.11.1b1->9.11.1rc1, and 9.9.9-S8.
CVE-2017-3138	named contains a feature which allows operators to issue commands to a running server by communicating with the server process over a control channel, using a utility program such as rndc. A regression introduced in a recent feature change has created a situation under which some versions of named can be caused to exit with a REQUIRE assertion failure if they are sent a null command string. Affects BIND 9.9.9->9.9.9-P7, 9.9.10b1->9.9.10rc2, 9.10.4->9.10.4-P7, 9.10.5b1->9.10.5rc2, 9.11.0->9.11.0-P4, 9.11.1b1->9.11.1rc2, 9.9.9-S1->9.9.9-S9.
CVE-2017-3142	An attacker who is able to send and receive messages to an authoritative DNS server and who has knowledge of a valid TSIG key name may be able to circumvent TSIG authentication of AXFR requests via a carefully constructed request packet. A server that relies solely on TSIG keys for protection with no other ACL protection could be manipulated into: providing an AXFR of a zone to an unauthorized recipient or accepting bogus NOTIFY packets. Affects BIND 9.4.0->9.8.8, 9.9.0->9.9.10-P1, 9.10.0->9.10.5-P1, 9.11.0->9.11.1-P1, 9.9.3-S1->9.9.10-S2, 9.10.5-S1->9.10.5-S2.
CVE-2017-3143	An attacker who is able to send and receive messages to an authoritative DNS server and who has knowledge of a valid TSIG key name for the zone and service being targeted may be able to manipulate BIND into accepting an unauthorized dynamic update. Affects BIND 9.4.0->9.8.8, 9.9.0->9.9.10-P1, 9.10.0->9.10.5-

	P1, 9.11.0->9.11.1-P1, 9.9.3-S1->9.9.10-S2, 9.10.5-S1->9.10.5-S2.
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-2017-3157	By exploiting the way Apache OpenOffice before 4.1.4 renders embedded objects, an attacker could craft a document that allows reading in a file from the user's filesystem. Information could be retrieved by the attacker by, e.g., using hidden sections to store the information, tricking the user into saving the document and convincing the user to send the document back to the attacker. The vulnerability is mitigated by the need for the attacker to know the precise file path in the target system, and the need to trick the user into saving the document and sending it back.
CVE-2017-3167	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, use of the ap_get_basic_auth_pw() by third-party modules outside of the authentication phase may lead to authentication requirements being bypassed.
CVE-2017-3169	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.
CVE-2017-3231	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the

	Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS v3.0 Base Score 4.3 (Confidentiality impacts).
CVE-2017-3238	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).
CVE-2017-3241	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: RMI). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability can only be exploited by supplying data to APIs in the specified Component without using Untrusted Java Web Start applications or Untrusted Java applets, such as through a web service. CVSS v3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts).
CVE-2017-3243	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Charsets). Supported versions that are affected are 5.5.53 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.4 (Availability impacts).
CVE-2017-3244	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang

	or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).
CVE-2017-3251	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.16 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 v3.0 Base Score 4.9 (Availability impacts).
CVE-2017-3252	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JAAS). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS v3.0 Base Score 5.8 (Integrity impacts).
CVE-2017-3253	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: 2D). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111; JRockit: R28.3.12. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start

	applications or sandboxed Java applets, such as through a web service. CVSS v3.0 Base Score 7.5 (Availability impacts).
CVE-2017-3256	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).
CVE-2017-3258	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).
CVE-2017-3261	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS v3.0 Base Score 4.3 (Confidentiality impacts).
CVE-2017-3265	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks

	require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 5.6 (Confidentiality and Availability impacts).
CVE-2017-3272	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 6u131, 7u121 and 8u112; Java SE Embedded: 8u111. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS v3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts).
CVE-2017-3273	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).
CVE-2017-3289	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 7u121 and 8u112; Java SE Embedded: 8u111. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of

	this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS v3.0 Base Score 9.6 (Confidentiality, Integrity and Availability impacts).
CVE-2017-3291	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS v3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts).
CVE-2017-3302	Crash in libmysqlclient.so in Oracle MySQL before 5.6.21 and 5.7.x before 5.7.5 and MariaDB through 5.5.54, 10.0.x through 10.0.29, 10.1.x through 10.1.21, and 10.2.x through 10.2.3.
CVE-2017-3305	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: C API). Supported versions that are affected are 5.5.55 and earlier and 5.6.35 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 access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 5.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N). NOTE: the previous information is from the April 2017 CPU. Oracle has not commented on third-party claims that this issue allows man-in-the-middle attackers to hijack the authentication of users by leveraging incorrect ordering of security parameter verification in a client, aka, "The Riddle".
CVE-2017-3308	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products.

	Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).
CVE-2017-3309	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).
CVE-2017-3312	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS v3.0 Base Score 6.7 (Confidentiality, Integrity and Availability impacts).
CVE-2017-3313	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: MyISAM). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS v3.0 Base Score 4.7 (Confidentiality impacts).
CVE-2017-3317	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Logging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability

	can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.0 (Availability impacts).
CVE-2017-3318	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Error Handling). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS v3.0 Base Score 4.0 (Confidentiality impacts).
CVE-2017-3319	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: X Plugin). Supported versions that are affected are 5.7.16 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 read access to a subset of MySQL Server accessible data. CVSS v3.0 Base Score 3.1 (Confidentiality impacts).
CVE-2017-3320	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.7.16 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS v3.0 Base Score 2.4 (Confidentiality impacts).
CVE-2017-3329	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Thread Pooling). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3331	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). The

	supported version that is affected is 5.7.11 to 5.7.17. 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-2017-3450	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3453	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3454	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2017-3455	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful

	attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 5.4 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N).
CVE-2017-3456	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3457	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3458	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3459	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability

	impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3460	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Audit Plug-in). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3461	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3462	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3463	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3464	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported

	versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2017-3465	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2017-3467	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: C API). Supported versions that are affected are 5.7.17 and earlier. 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 read access to a subset of MySQL Server 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-2017-3468	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.7.17 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-2017-3509	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some

	of Java SE, Java SE Embedded accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:L/A:N).
CVE-2017-3511	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JCE). Supported versions that are affected are Java SE: 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where Java SE, Java SE Embedded, JRockit executes to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2017-3526	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JAXP). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed

	Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3529	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: UDF). Supported versions that are affected are 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 ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3533	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via FTP to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2017-3539	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets, that load and

	run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:L/A:N).
CVE-2017-3544	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u141, 7u131 and 8u121; Java SE Embedded: 8u121; JRockit: R28.3.13. Difficult to exploit vulnerability allows unauthenticated attacker with network access via SMTP to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2017-3599	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Pluggable Auth). Supported versions that are affected are 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). NOTE: the previous information is from the April 2017 CPU. Oracle has not commented on third-party claims that this issue is an integer overflow in sql/auth/sql_authentication.cc which allows remote attackers to cause a denial of service via a crafted authentication packet.
CVE-2017-3600	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server.

	Note: CVE-2017-3600 is equivalent to CVE-2016-5483. CVSS 3.0 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2017-3633	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows unauthenticated attacker with network access via Memcached to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:H).
CVE-2017-3634	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.6.36 and earlier and 5.7.18 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3635	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/C). Supported versions that are affected are 6.1.10 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors. Note: The documentation has also been updated for the correct way to use mysql_stmt_close(). Please see: https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-execute.html, https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-fetch.html, https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-close.html, https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-error.html, https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-errno.html, and https://dev.mysql.com/doc/refman/5.7/en/mysql-stmt-sqlstate.html. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVE-2017-3636	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.56 and earlier and 5.6.36 and earlier. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).
CVE-2017-3637	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: X Plugin). Supported versions that are affected are 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 ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3638	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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-2017-3639	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 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-2017-3640	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 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-2017-3641	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-2017-3642	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 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-2017-3643	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 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-2017-3644	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 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-2017-3645	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3647	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3648	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Charsets). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3649	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3650	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: C API). Supported versions

	that are affected are 5.7.18 and earlier. 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 read access to a subset of MySQL Server 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-2017-3651	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2017-3652	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N).
CVE-2017-3653	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2017-3731	If an SSL/TLS server or client is running on a 32-bit host, and a specific cipher is being used, then a truncated packet can cause that server or client to perform an out-of-bounds read, usually resulting in a crash. For OpenSSL 1.1.0, the crash can be triggered when using CHACHA20/POLY1305; users should upgrade to 1.1.0d. For Openssl 1.0.2, the crash can be

	triggered when using RC4-MD5; users who have not disabled that algorithm should update to 1.0.2k.
CVE-2017-3732	There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL 1.0.2 before 1.0.2k and 1.1.0 before 1.1.0d. 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. For example this can occur by default in OpenSSL DHE based SSL/TLS ciphersuites. Note: This issue is very similar to CVE-2015-3193 but must be treated as a separate problem.
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	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.
CVE-2017-3737	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.
CVE-2017-3738	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 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-2017-5193	The nickcmp function in Irssi before 0.8.21 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a message without a nick.
CVE-2017-5194	Use-after-free vulnerability in Irssi before 0.8.21 allows remote attackers to cause a denial of service (crash) via an invalid nick message.

CVE-2017-5195	Irssi 0.8.17 before 0.8.21 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted ANSI x8 color code.
CVE-2017-5196	Irssi 0.8.18 before 0.8.21 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via vectors involving strings that are not UTF8.
CVE-2017-5202	The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in print-isoclns.c:clnp_print().
CVE-2017-5203	The BOOTP parser in tcpdump before 4.9.0 has a buffer overflow in print-bootp.c:bootp_print().
CVE-2017-5204	The IPv6 parser in tcpdump before 4.9.0 has a buffer overflow in print-ip6.c:ip6_print().
CVE-2017-5205	The ISAKMP parser in tcpdump before 4.9.0 has a buffer overflow in print-isakmp.c:ikev2_e_print().
CVE-2017-5225	LibTIFF version 4.0.7 is vulnerable to a heap buffer overflow in the tools/tiffcp resulting in DoS or code execution via a crafted BitsPerSample value.
CVE-2017-5334	Double free vulnerability in the gnutls_x509_ext_import_proxy function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via crafted policy language information in an X.509 certificate with a Proxy Certificate Information extension.
CVE-2017-5335	The stream reading functions in lib/opencdk/read-packet.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to cause a denial of service (out-of-memory error and crash) via a crafted OpenPGP certificate.
CVE-2017-5336	Stack-based buffer overflow in the cdk_pk_get_keyid function in lib/opencdk/pubkey.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via a crafted OpenPGP certificate.
CVE-2017-5337	Multiple heap-based buffer overflows in the read_attribute function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to have unspecified impact via a crafted OpenPGP certificate.
CVE-2017-5340	Zend/zend_hash.c in PHP before 7.0.15 and 7.1.x before 7.1.1 mishandles certain cases that require large array allocations, which allows remote attackers to execute arbitrary code or cause a denial of service (integer overflow, uninitialized memory access, and use of arbitrary destructor function pointers) via crafted serialized data.
CVE-2017-5341	The OTV parser in tcpdump before 4.9.0 has a buffer overflow in print-otv.c:otv_print().
CVE-2017-5342	In tcpdump before 4.9.0, a bug in multiple protocol parsers (Geneve, GRE, NSH, OTV, VXLAN and

	VXLAN GPE) could cause a buffer overflow in print-ether.c:ether_print().
CVE-2017-5356	Irssi before 0.8.21 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a string containing a formatting sequence (%[) without a closing bracket (]).
CVE-2017-5373	Memory safety bugs were reported in Firefox 50.1 and Firefox ESR 45.6. 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 < 45.7, Firefox ESR < 45.7, and Firefox < 51.
CVE-2017-5374	Memory safety bugs were reported in Firefox 50.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 51.
CVE-2017-5375	JIT code allocation can allow for a bypass of ASLR and DEP protections leading to potential memory corruption attacks. This vulnerability affects Thunderbird < 45.7, Firefox ESR < 45.7, and Firefox < 51.
CVE-2017-5376	Use-after-free while manipulating XSL in XSLT documents. This vulnerability affects Thunderbird < 45.7, Firefox ESR < 45.7, and Firefox < 51.
CVE-2017-5377	A memory corruption vulnerability in Skia that can occur when using transforms to make gradients, resulting in a potentially exploitable crash. This vulnerability affects Firefox < 51.
CVE-2017-5378	Hashed codes of JavaScript objects are shared between pages. This allows for pointer leaks because an object's address can be discovered through hash codes, and also allows for data leakage of an object's content using these hash codes. This vulnerability affects Thunderbird < 45.7, Firefox ESR < 45.7, and Firefox < 51.
CVE-2017-5379	Use-after-free vulnerability in Web Animations when interacting with cycle collection found through fuzzing. This vulnerability affects Firefox < 51.
CVE-2017-5380	A potential use-after-free found through fuzzing during DOM manipulation of SVG content. This vulnerability affects Thunderbird < 45.7, Firefox ESR < 45.7, and Firefox < 51.
CVE-2017-5381	The "export" function in the Certificate Viewer can force local filesystem navigation when the "common name" in a certificate contains slashes, allowing certificate content to be saved in unsafe locations with an arbitrary filename. This vulnerability affects Firefox < 51.

CVE-2017-5382	Feed preview for RSS feeds can be used to capture errors and exceptions generated by privileged content, allowing for the exposure of internal information not meant to be seen by web content. This vulnerability affects Firefox < 51.
CVE-2017-5383	URLs containing certain unicode glyphs for alternative hyphens and quotes do not properly trigger punycode display, allowing for domain name spoofing attacks in the location bar. This vulnerability affects Thunderbird < 45.7, Firefox ESR < 45.7, and Firefox < 51.
CVE-2017-5384	Proxy Auto-Config (PAC) files can specify a JavaScript function called for all URL requests with the full URL path which exposes more information than would be sent to the proxy itself in the case of HTTPS. Normally the Proxy Auto-Config file is specified by the user or machine owner and presumed to be non-malicious, but if a user has enabled Web Proxy Auto Detect (WPAD) this file can be served remotely. This vulnerability affects Firefox < 51.
CVE-2017-5385	Data sent with in multipart channels, such as the multipart/x-mixed-replace MIME type, will ignore the referrer-policy response header, leading to potential information disclosure for sites using this header. This vulnerability affects Firefox < 51.
CVE-2017-5386	WebExtension scripts can use the "data:" protocol to affect pages loaded by other web extensions using this protocol, leading to potential data disclosure or privilege escalation in affected extensions. This vulnerability affects Firefox ESR < 45.7 and Firefox < 51.
CVE-2017-5387	The existence of a specifically requested local file can be found due to the double firing of the "onerror" when the "source" attribute on a "<track>" tag refers to a file that does not exist if the source page is loaded locally. This vulnerability affects Firefox < 51.
CVE-2017-5388	A STUN server in conjunction with a large number of "webkitRTCPeerConnection" objects can be used to send large STUN packets in a short period of time due to a lack of rate limiting being applied on e10s systems, allowing for a denial of service attack. This vulnerability affects Firefox < 51.
CVE-2017-5389	WebExtensions could use the "mozAddonManager" API by modifying the CSP headers on sites with the appropriate permissions and then using host requests to redirect script loads to a malicious site. This allows a malicious extension to then install additional extensions without explicit user permission. This vulnerability affects Firefox < 51.
CVE-2017-5390	The JSON viewer in the Developer Tools uses insecure methods to create a communication channel for copying and viewing JSON or HTTP headers data, allowing for

	potential privilege escalation. This vulnerability affects Thunderbird < 45.7, Firefox ESR < 45.7, and Firefox < 51.
CVE-2017-5391	Special "about:" pages used by web content, such as RSS feeds, can load privileged "about:" pages in an iframe. If a content-injection bug were found in one of those pages this could allow for potential privilege escalation. This vulnerability affects Firefox < 51.
CVE-2017-5393	The "mozAddonManager" allows for the installation of extensions from the CDN for addons.mozilla.org, a publicly accessible site. This could allow malicious extensions to install additional extensions from the CDN in combination with an XSS attack on Mozilla AMO sites. This vulnerability affects Firefox < 51.
CVE-2017-5396	A use-after-free vulnerability in the Media Decoder when working with media files when some events are fired after the media elements are freed from memory. This vulnerability affects Thunderbird < 45.7, Firefox ESR < 45.7, and Firefox < 51.
CVE-2017-5398	Memory safety bugs were reported in Thunderbird 45.7. 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 < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.
CVE-2017-5399	Memory safety bugs were reported in Firefox 51. 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 < 52 and Thunderbird < 52.
CVE-2017-5400	JIT-spray targeting asm.js combined with a heap spray allows for a bypass of ASLR and DEP protections leading to potential memory corruption attacks. This vulnerability affects Firefox < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.
CVE-2017-5401	A crash triggerable by web content in which an "ErrorResult" references unassigned memory due to a logic error. The resulting crash may be exploitable. This vulnerability affects Firefox < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.
CVE-2017-5402	A use-after-free can occur when events are fired for a "FontFace" object after the object has been already been destroyed while working with fonts. This results in a potentially exploitable crash. This vulnerability affects Firefox < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.
CVE-2017-5403	When adding a range to an object in the DOM, it is possible to use "addRange" to add the range to an incorrect root object. This triggers a use-after-

	free, resulting in a potentially exploitable crash. This vulnerability affects Firefox < 52 and Thunderbird < 52.
CVE-2017-5404	A use-after-free error can occur when manipulating ranges in selections with one node inside a native anonymous tree and one node outside of it. This results in a potentially exploitable crash. This vulnerability affects Firefox < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.
CVE-2017-5405	Certain response codes in FTP connections can result in the use of uninitialized values for ports in FTP operations. This vulnerability affects Firefox < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.
CVE-2017-5406	A segmentation fault can occur in the Skia graphics library during some canvas operations due to issues with mask/clip intersection and empty masks. This vulnerability affects Firefox < 52 and Thunderbird < 52.
CVE-2017-5407	Using SVG filters that don't use the fixed point math implementation on a target iframe, a malicious page can extract pixel values from a targeted user. This can be used to extract history information and read text values across domains. This violates same-origin policy and leads to information disclosure. This vulnerability affects Firefox < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.
CVE-2017-5408	Video files loaded video captions cross-origin without checking for the presence of CORS headers permitting such cross-origin use, leading to potential information disclosure for video captions. This vulnerability affects Firefox < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.
CVE-2017-5410	Memory corruption resulting in a potentially exploitable crash during garbage collection of JavaScript due errors in how incremental sweeping is managed for memory cleanup. This vulnerability affects Firefox < 52, Firefox ESR < 45.8, Thunderbird < 52, and Thunderbird < 45.8.
CVE-2017-5412	A buffer overflow read during SVG filter color value operations, resulting in data exposure. This vulnerability affects Firefox < 52 and Thunderbird < 52.
CVE-2017-5413	A segmentation fault can occur during some bidirectional layout operations. This vulnerability affects Firefox < 52 and Thunderbird < 52.
CVE-2017-5414	The file picker dialog can choose and display the wrong local default directory when instantiated. On some operating systems, this can lead to information disclosure, such as the operating system or the local account name. This vulnerability affects Firefox < 52 and Thunderbird < 52.

CVE-2017-5415	An attack can use a blob URL and script to spoof an arbitrary addressbar URL prefaced by "blob:" as the protocol, leading to user confusion and further spoofing attacks. This vulnerability affects Firefox < 52.
CVE-2017-5416	In certain circumstances a networking event listener can be prematurely released. This appears to result in a null dereference in practice. This vulnerability affects Firefox < 52 and Thunderbird < 52.
CVE-2017-5417	When dragging content from the primary browser pane to the addressbar on a malicious site, it is possible to change the addressbar so that the displayed location following navigation does not match the URL of the newly loaded page. This allows for spoofing attacks. This vulnerability affects Firefox < 52.
CVE-2017-5418	An out of bounds read error occurs when parsing some HTTP digest authorization responses, resulting in information leakage through the reading of random memory containing matches to specifically set patterns. This vulnerability affects Firefox < 52 and Thunderbird < 52.
CVE-2017-5419	If a malicious site repeatedly triggers a modal authentication prompt, eventually the browser UI will become non-responsive, requiring shutdown through the operating system. This is a denial of service (DOS) attack. This vulnerability affects Firefox < 52 and Thunderbird < 52.
CVE-2017-5420	A "javascript:" url loaded by a malicious page can obfuscate its location by blanking the URL displayed in the addressbar, allowing for an attacker to spoof an existing page without the malicious page's address being displayed correctly. This vulnerability affects Firefox < 52.
CVE-2017-5421	A malicious site could spoof the contents of the print preview window if popup windows are enabled, resulting in user confusion of what site is currently loaded. This vulnerability affects Firefox < 52 and Thunderbird < 52.
CVE-2017-5422	If a malicious site uses the "view-source:" protocol in a series within a single hyperlink, it can trigger a non-exploitable browser crash when the hyperlink is selected. This was fixed by no longer making "view-source:" linkable. This vulnerability affects Firefox < 52 and Thunderbird < 52.
CVE-2017-5426	On Linux, if the secure computing mode BPF (seccomp-bpf) filter is running when the Gecko Media Plugin sandbox is started, the sandbox fails to be applied and items that would run within the sandbox are run protected only by the running filter which is typically weak compared to the sandbox. Note: this issue only affects Linux. Other operating systems are not affected.

	This vulnerability affects Firefox < 52 and Thunderbird < 52.
CVE-2017-5427	A non-existent chrome.manifest file will attempt to be loaded during startup from the primary installation directory. If a malicious user with local access puts chrome.manifest and other referenced files in this directory, they will be loaded and activated during startup. This could result in malicious software being added without consent or modification of referenced installed files. This vulnerability affects Firefox < 52.
CVE-2017-5428	An integer overflow in "createImageBitmap()" was reported through the Pwn2Own contest. The fix for this vulnerability disables the experimental extensions to the "createImageBitmap" API. This function runs in the content sandbox, requiring a second vulnerability to compromise a user's computer. This vulnerability affects Firefox ESR < 52.0.1 and Firefox < 52.0.1.
CVE-2017-5429	Memory safety bugs were reported in Firefox 52, Firefox ESR 45.8, Firefox ESR 52, and Thunderbird 52. 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 < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5430	Memory safety bugs were reported in Firefox 52, Firefox ESR 52, and Thunderbird 52. 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 < 52.1, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5432	A use-after-free vulnerability occurs during certain text input selection resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5433	A use-after-free vulnerability in SMIL animation functions occurs when pointers to animation elements in an array are dropped from the animation controller while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5434	A use-after-free vulnerability occurs when redirecting focus handling which results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5435	A use-after-free vulnerability occurs during transaction processing in the editor during design mode

	interactions. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5436	An out-of-bounds write in the Graphite 2 library triggered with a maliciously crafted Graphite font. This results in a potentially exploitable crash. This issue was fixed in the Graphite 2 library as well as Mozilla products. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5438	A use-after-free vulnerability during XSLT processing due to the result handler being held by a freed handler during handling. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5439	A use-after-free vulnerability during XSLT processing due to poor handling of template parameters. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5440	A use-after-free vulnerability during XSLT processing due to a failure to propagate error conditions during matching while evaluating context, leading to objects being used when they no longer exist. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5441	A use-after-free vulnerability when holding a selection during scroll events. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5442	A use-after-free vulnerability during changes in style when manipulating DOM elements. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5443	An out-of-bounds write vulnerability while decoding improperly formed BinHex format archives. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5444	A buffer overflow vulnerability while parsing "application/http-index-format" format content when the header contains improperly formatted data. This allows for an out-of-bounds read of data from memory. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.

CVE-2017-5445	A vulnerability while parsing "application/http-index-format" format content where uninitialized values are used to create an array. This could allow the reading of uninitialized memory into the arrays affected. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5446	An out-of-bounds read when an HTTP/2 connection to a servers sends "DATA" frames with incorrect data content. This leads to a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5447	An out-of-bounds read during the processing of glyph widths during text layout. This results in a potentially exploitable crash and could allow an attacker to read otherwise inaccessible memory. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5448	An out-of-bounds write in "ClearKeyDecryptor" while decrypting some Clearkey-encrypted media content. The "ClearKeyDecryptor" code runs within the Gecko Media Plugin (GMP) sandbox. If a second mechanism is found to escape the sandbox, this vulnerability allows for the writing of arbitrary data within memory, resulting in a potentially exploitable crash. This vulnerability affects Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5449	A possibly exploitable crash triggered during layout and manipulation of bidirectional unicode text in concert with CSS animations. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5451	A mechanism to spoof the addressbar through the user interaction on the addressbar and the "onblur" event. The event could be used by script to affect text display to make the loaded site appear to be different from the one actually loaded within the addressbar. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5453	A mechanism to inject static HTML into the RSS reader preview page due to a failure to escape characters sent as URL parameters for a feed's "TITLE" element. This vulnerability allows for spoofing but no scripted content can be run. This vulnerability affects Firefox < 53.
CVE-2017-5454	A mechanism to bypass file system access protections in the sandbox to use the file picker to access different files than those selected in the file picker through the use of relative paths. This allows for read only access to the local file system. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 52.1, and Firefox < 53.

CVE-2017-5455	The internal feed reader APIs that crossed the sandbox barrier allowed for a sandbox escape and escalation of privilege if combined with another vulnerability that resulted in remote code execution inside the sandboxed process. This vulnerability affects Firefox ESR < 52.1 and Firefox < 53.
CVE-2017-5456	A mechanism to bypass file system access protections in the sandbox using the file system request constructor through an IPC message. This allows for read and write access to the local file system. This vulnerability affects Firefox ESR < 52.1 and Firefox < 53.
CVE-2017-5458	When a "javascript:" URL is drag and dropped by a user into the addressbar, the URL will be processed and executed. This allows for users to be socially engineered to execute an XSS attack on themselves. This vulnerability affects Firefox < 53.
CVE-2017-5459	A buffer overflow in WebGL triggerable by web content, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5460	A use-after-free vulnerability in frame selection triggered by a combination of malicious script content and key presses by a user. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5461	Mozilla Network Security Services (NSS) before 3.21.4, 3.22.x through 3.28.x before 3.28.4, 3.29.x before 3.29.5, and 3.30.x before 3.30.1 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by leveraging incorrect base64 operations.
CVE-2017-5462	A flaw in DRBG number generation within the Network Security Services (NSS) library where the internal state V does not correctly carry bits over. The NSS library has been updated to fix this issue to address this issue and Firefox ESR 52.1 has been updated with NSS version 3.28.4. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5464	During DOM manipulations of the accessibility tree through script, the DOM tree can become out of sync with the accessibility tree, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5465	An out-of-bounds read while processing SVG content in "ConvolvePixel". This results in a crash and also allows for otherwise inaccessible memory being copied into SVG graphic content, which could then displayed. This

	vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5466	If a page is loaded from an original site through a hyperlink and contains a redirect to a "data:text/html" URL, triggering a reload will run the reloaded "data:text/html" page with its origin set incorrectly. This allows for a cross-site scripting (XSS) attack. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5467	A potential memory corruption and crash when using Skia content when drawing content outside of the bounds of a clipping region. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5468	An issue with incorrect ownership model of "privateBrowsing" information exposed through developer tools. This can result in a non-exploitable crash when manually triggered during debugging. This vulnerability affects Firefox < 53.
CVE-2017-5469	Fixed potential buffer overflows in generated Firefox code due to CVE-2016-6354 issue in Flex. This vulnerability affects Thunderbird < 52.1, Firefox ESR < 45.9, Firefox ESR < 52.1, and Firefox < 53.
CVE-2017-5470	Memory safety bugs were reported in Firefox 53 and Firefox ESR 52.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-5471	Memory safety bugs were reported in Firefox 53. 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 < 54.
CVE-2017-5472	A use-after-free vulnerability with the frameloader during tree reconstruction while regenerating CSS layout when attempting to use a node in the tree that no longer exists. This results in a potentially exploitable crash. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-5482	The Q.933 parser in tcpdump before 4.9.0 has a buffer overflow in print-fr.c:q933_print(), a different vulnerability than CVE-2016-8575.
CVE-2017-5483	The SNMP parser in tcpdump before 4.9.0 has a buffer overflow in print-snmp.c:asn1_parse().
CVE-2017-5484	The ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-atm.c:sig_print().
CVE-2017-5485	The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in addrtoname.c:lookup_nsap().

CVE-2017-5486	The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in print-isoclns.c:clnp_print().
CVE-2017-5495	All versions of Quagga, 0.93 through 1.1.0, are vulnerable to an unbounded memory allocation in the telnet 'vty' CLI, leading to a Denial-of-Service of Quagga daemons, or even the entire host. When Quagga daemons are configured with their telnet CLI enabled, anyone who can connect to the TCP ports can trigger this vulnerability, prior to authentication. Most distributions restrict the Quagga telnet interface to local access only by default. The Quagga telnet interface 'vty' input buffer grows automatically, without bound, so long as a newline is not entered. This allows an attacker to cause the Quagga daemon to allocate unbounded memory by sending very long strings without a newline. Eventually the daemon is terminated by the system, or the system itself runs out of memory. This is fixed in Quagga 1.1.1 and Free Range Routing (FRR) Protocol Suite 2017-01-10.
CVE-2017-5506	Double free vulnerability in magick/profile.c in ImageMagick allows remote attackers to have unspecified impact via a crafted file.
CVE-2017-5507	Memory leak in coders/mpc.c in ImageMagick before 6.9.7-4 and 7.x before 7.0.4-4 allows remote attackers to cause a denial of service (memory consumption) via vectors involving a pixel cache.
CVE-2017-5508	Heap-based buffer overflow in the PushQuantumPixel function in ImageMagick before 6.9.7-3 and 7.x before 7.0.4-3 allows remote attackers to cause a denial of service (application crash) via a crafted TIFF file.
CVE-2017-5510	coders/psd.c in ImageMagick allows remote attackers to have unspecified impact via a crafted PSD file, which triggers an out-of-bounds write.
CVE-2017-5511	coders/psd.c in ImageMagick allows remote attackers to have unspecified impact by leveraging an improper cast, which triggers a heap-based buffer overflow.
CVE-2017-5525	Memory leak in hw/audio/ac97.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption and QEMU process crash) via a large number of device unplug operations.
CVE-2017-5526	Memory leak in hw/audio/es1370.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption and QEMU process crash) via a large number of device unplug operations.
CVE-2017-5546	The freelist-randomization feature in mm/slab.c in the Linux kernel 4.8.x and 4.9.x before 4.9.5 allows local users to cause a denial of service (duplicate freelist entries and system crash) or possibly have

	unspecified other impact in opportunistic circumstances by leveraging the selection of a large value for a random number.
CVE-2017-5549	The klsi_105_get_line_state function in drivers/usb/serial/kl5kusb105.c in the Linux kernel before 4.9.5 places uninitialized heap-memory contents into a log entry upon a failure to read the line status, which allows local users to obtain sensitive information by reading the log.
CVE-2017-5550	Off-by-one error in the pipe_advance function in lib/iov_iter.c in the Linux kernel before 4.9.5 allows local users to obtain sensitive information from uninitialized heap-memory locations in opportunistic circumstances by reading from a pipe after an incorrect buffer-release decision.
CVE-2017-5551	The simple_set_acl function in fs/posix_acl.c in the Linux kernel before 4.9.6 preserves the setgid bit during a setxattr call involving a tmpfs filesystem, which allows local users to gain group privileges by leveraging the existence of a setgid program with restrictions on execute permissions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-7097.
CVE-2017-5552	Memory leak in the virgl_resource_attach_backing function in hw/display/virtio-gpu-3d.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (host memory consumption) via a large number of VIRTIO_GPU_CMD_RESOURCE_ATTACH_BACKING commands.
CVE-2017-5563	LibTIFF version 4.0.7 is vulnerable to a heap-based buffer over-read in tif_lzw.c resulting in DoS or code execution via a crafted bmp image to tools/bmp2tiff.
CVE-2017-5576	Integer overflow in the vc4_get_bcl function in drivers/gpu/drm/vc4/vc4_gem.c in the VideoCore DRM driver in the Linux kernel before 4.9.7 allows local users to cause a denial of service or possibly have unspecified other impact via a crafted size value in a VC4_SUBMIT_CL ioctl call.
CVE-2017-5577	The vc4_get_bcl function in drivers/gpu/drm/vc4/vc4_gem.c in the VideoCore DRM driver in the Linux kernel before 4.9.7 does not set an errno value upon certain overflow detections, which allows local users to cause a denial of service (incorrect pointer dereference and OOPS) via inconsistent size values in a VC4_SUBMIT_CL ioctl call.
CVE-2017-5578	Memory leak in the virtio_gpu_resource_attach_backing function in hw/display/virtio-gpu.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (host memory consumption) via a large number of

	VIRTIO_GPU_CMD_RESOURCE_ATTACH_BACKING commands.
CVE-2017-5579	Memory leak in the serial_exit_core function in hw/char/serial.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption and QEMU process crash) via a large number of device unplug operations.
CVE-2017-5601	An error in the lha_read_file_header_1() function (archive_read_support_format_lha.c) in libarchive 3.2.2 allows remote attackers to trigger an out-of-bounds read memory access and subsequently cause a crash via a specially crafted archive.
CVE-2017-5647	A bug in the handling of the pipelined requests in Apache Tomcat 9.0.0.M1 to 9.0.0.M18, 8.5.0 to 8.5.12, 8.0.0.RC1 to 8.0.42, 7.0.0 to 7.0.76, and 6.0.0 to 6.0.52, when send file was used, results in the pipelined request being lost when send file processing of the previous request completed. This could result in responses appearing to be sent for the wrong request. For example, a user agent that sent requests A, B and C could see the correct response for request A, the response for request C for request B and no response for request C.
CVE-2017-5648	While investigating bug 60718, it was noticed that some calls to application listeners in Apache Tomcat 9.0.0.M1 to 9.0.0.M17, 8.5.0 to 8.5.11, 8.0.0.RC1 to 8.0.41, and 7.0.0 to 7.0.75 did not use the appropriate facade object. When running an untrusted application under a SecurityManager, it was therefore possible for that untrusted application to retain a reference to the request or response object and thereby access and/or modify information associated with another web application.
CVE-2017-5664	The error page mechanism of the Java Servlet Specification requires that, when an error occurs and an error page is configured for the error that occurred, the original request and response are forwarded to the error page. This means that the request is presented to the error page with the original HTTP method. If the error page is a static file, expected behaviour is to serve content of the file as if processing a GET request, regardless of the actual HTTP method. The Default Servlet in Apache Tomcat 9.0.0.M1 to 9.0.0.M20, 8.5.0 to 8.5.14, 8.0.0.RC1 to 8.0.43 and 7.0.0 to 7.0.77 did not do this. Depending on the original request this could lead to unexpected and undesirable results for static error pages including, if the DefaultServlet is configured to permit writes, the replacement or removal of the custom error page. Notes for other user provided error pages: (1) Unless explicitly coded otherwise, JSPs ignore the HTTP method. JSPs used as error pages

	must must ensure that they handle any error dispatch as a GET request, regardless of the actual method. (2) By default, the response generated by a Servlet does depend on the HTTP method. Custom Servlets used as error pages must ensure that they handle any error dispatch as a GET request, regardless of the actual method.
CVE-2017-5667	The sdhci_sdma_transfer_multi_blocks function in hw/sd/sdhci.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (out-of-bounds heap access and crash) or execute arbitrary code on the QEMU host via vectors involving the data transfer length.
CVE-2017-5669	The do_shmat function in ipc/shm.c in the Linux kernel through 4.9.12 does not restrict the address calculated by a certain rounding operation, which allows local users to map page zero, and consequently bypass a protection mechanism that exists for the mmap system call, by making crafted shmget and shmat system calls in a privileged context.
CVE-2017-5715	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-2017-5753	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-2017-5837	The gst_riff_create_audio_caps function in gst-libs/gst/riff/riff-media.c in gst-plugins-base in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (floating point exception and crash) via a crafted video file.
CVE-2017-5839	The gst_riff_create_audio_caps function in gst-libs/gst/riff/riff-media.c in gst-plugins-base in GStreamer before 1.10.3 does not properly limit recursion, which allows remote attackers to cause a denial of service (stack overflow and crash) via vectors involving nested WAVEFORMATEX.
CVE-2017-5840	The qtdemux_parse_samples function in gst/isomp4/qtdemux.c in gst-plugins-good in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (out-of-bounds heap read) via vectors involving the current stts index.

CVE-2017-5841	The gst_avi_demux_parse_ncdt function in gst/avi/gstavidemux.c in gst-plugins-good in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (out-of-bounds heap read) via vectors involving ncdt tags.
CVE-2017-5842	The html_context_handle_element function in gst/subparse/samiparse.c in gst-plugins-base in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted SMI file, as demonstrated by OneNote_Manager.smi.
CVE-2017-5844	The gst_riff_create_audio_caps function in gst-libs/gst/riff/riff-media.c in gst-plugins-base in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (floating point exception and crash) via a crafted ASF file.
CVE-2017-5845	The gst_avi_demux_parse_ncdt function in gst/avi/gstavidemux.c in gst-plugins-good in GStreamer before 1.10.3 allows remote attackers to cause a denial of service (invalid memory read and crash) via a ncdt sub-tag that "goes behind" the surrounding tag.
CVE-2017-5856	Memory leak in the megasas_handle_dcmd function in hw/scsi/megasas.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption) via MegaRAID Firmware Interface (MFI) commands with the sglist size set to a value over 2 Gb.
CVE-2017-5857	Memory leak in the virgl_cmd_resource_unref function in hw/display/virtio-gpu-3d.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of service (host memory consumption) via a large number of VIRTIO_GPU_CMD_RESOURCE_UNREF commands sent without detaching the backing storage beforehand.
CVE-2017-5897	The ip6gre_err function in net/ipv6/ip6_gre.c in the Linux kernel allows remote attackers to have unspecified impact via vectors involving GRE flags in an IPv6 packet, which trigger an out-of-bounds access.
CVE-2017-5898	Integer overflow in the emulated_apdu_from_guest function in usb/dev-smartcard-reader.c in Quick Emulator (Qemu), when built with the CCID Card device emulator support, allows local users to cause a denial of service (application crash) via a large Application Protocol Data Units (APDU) unit.
CVE-2017-5932	The path autocompletion feature in Bash 4.4 allows local users to gain privileges via a crafted filename starting with a " (double quote) character and a command substitution metacharacter.
CVE-2017-5934	Cross-site scripting (XSS) vulnerability in the link dialogue in GUI editor in MoinMoin before 1.9.10 allows

	remote attackers to inject arbitrary web script or HTML via unspecified vectors.
CVE-2017-5936	OpenStack Nova-LXD before 13.1.1 uses the wrong name for the veth pairs when applying Neutron security group rules for instances, which allows remote attackers to bypass intended security restrictions.
CVE-2017-5951	The mem_get_bits_rectangle function in base/gdevmem.c in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file.
CVE-2017-5970	The ipv4_pktinfo_prepare function in net/ipv4/ip_sockglue.c in the Linux kernel through 4.9.9 allows attackers to cause a denial of service (system crash) via (1) an application that makes crafted system calls or possibly (2) IPv4 traffic with invalid IP options.
CVE-2017-5973	The xhci_kick_epctx function in hw/usb/hcd-xhci.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (infinite loop and QEMU process crash) via vectors related to control transfer descriptor sequence.
CVE-2017-5974	Heap-based buffer overflow in the __zzip_get32 function in fetch.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (crash) via a crafted ZIP file.
CVE-2017-5975	Heap-based buffer overflow in the __zzip_get64 function in fetch.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (crash) via a crafted ZIP file.
CVE-2017-5976	Heap-based buffer overflow in the zzip_mem_entry_extra_block function in memdisk.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (crash) via a crafted ZIP file.
CVE-2017-5977	The zzip_mem_entry_extra_block function in memdisk.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (invalid memory read and crash) via a crafted ZIP file.
CVE-2017-5978	The zzip_mem_entry_new function in memdisk.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted ZIP file.
CVE-2017-5979	The prescan_entry function in fseeko.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted ZIP file.
CVE-2017-5980	The zzip_mem_entry_new function in memdisk.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted ZIP file.

CVE-2017-5981	seeko.c in zziplib 0.13.62 allows remote attackers to cause a denial of service (assertion failure and crash) via a crafted ZIP file.
CVE-2017-5985	lxc-user-nic in Linux Containers (LXC) allows local users with a lxc-usernet allocation to create network interfaces on the host and choose the name of those interfaces by leveraging lack of netns ownership check.
CVE-2017-5986	Race condition in the sctp_wait_for_sndbuf function in net/sctp/socket.c in the Linux kernel before 4.9.11 allows local users to cause a denial of service (assertion failure and panic) via a multithreaded application that peels off an association in a certain buffer-full state.
CVE-2017-5987	The sdhci_sdma_transfer_multi_blocks function in hw/sd/sdhci.c in QEMU (aka Quick Emulator) allows local OS guest privileged users to cause a denial of service (infinite loop and QEMU process crash) via vectors involving the transfer mode register during multi block transfer.
CVE-2017-6001	Race condition in kernel/events/core.c in the Linux kernel before 4.9.7 allows local users to gain privileges via a crafted application that makes concurrent perf_event_open system calls for moving a software group into a hardware context. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-6786.
CVE-2017-6074	The dccp_rcv_state_process function in net/dccp/input.c in the Linux kernel through 4.9.11 mishandles DCCP_PKT_REQUEST packet data structures in the LISTEN state, which allows local users to obtain root privileges or cause a denial of service (double free) via an application that makes an IPV6_RECVPKTINFO setsockopt system call.
CVE-2017-6214	The tcp_splice_read function in net/ipv4/tcp.c in the Linux kernel before 4.9.11 allows remote attackers to cause a denial of service (infinite loop and soft lockup) via vectors involving a TCP packet with the URG flag.
CVE-2017-6257	NVIDIA GPU Display Driver contains a vulnerability in the kernel mode layer handler where a NULL pointer dereference may lead to denial of service or potential escalation of privileges
CVE-2017-6259	NVIDIA GPU Display Driver contains a vulnerability in the kernel mode layer handler where an incorrect detection and recovery from an invalid state produced by specific user actions may lead to denial of service.
CVE-2017-6266	NVIDIA GPU Display Driver contains a vulnerability in the kernel mode layer handler where improper access controls could allow unprivileged users to cause a denial of service.

CVE-2017-6267	NVIDIA GPU Display Driver contains a vulnerability in the kernel mode layer handler where an incorrect initialization of internal objects can cause an infinite loop which may lead to a denial of service.
CVE-2017-6272	NVIDIA GPU Display Driver contains a vulnerability in the kernel mode layer handler where a value passed from a user to the driver is not correctly validated and used as the index to an array which may lead to a denial of service or possible escalation of privileges.
CVE-2017-6298	An issue was discovered in ytnef before 1.9.1. This is related to a patch described as "1 of 9. Null Pointer Deref / calloc return value not checked."
CVE-2017-6311	gdk-pixbuf-thumbnailer.c in gdk-pixbuf allows context-dependent attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors related to printing an error message.
CVE-2017-6312	Integer overflow in io-ico.c in gdk-pixbuf allows context-dependent attackers to cause a denial of service (segmentation fault and application crash) via a crafted image entry offset in an ICO file, which triggers an out-of-bounds read, related to compiler optimizations.
CVE-2017-6313	Integer underflow in the load_resources function in io-icns.c in gdk-pixbuf allows context-dependent attackers to cause a denial of service (out-of-bounds read and program crash) via a crafted image entry size in an ICO file.
CVE-2017-6314	The make_available_at_least function in io-tiff.c in gdk-pixbuf allows context-dependent attackers to cause a denial of service (infinite loop) via a large TIFF file.
CVE-2017-6345	The LLC subsystem in the Linux kernel before 4.9.13 does not ensure that a certain destructor exists in required circumstances, which allows local users to cause a denial of service (BUG_ON) or possibly have unspecified other impact via crafted system calls.
CVE-2017-6346	Race condition in net/packet/af_packet.c in the Linux kernel before 4.9.13 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a multithreaded application that makes PACKET_FANOUT setsockopt system calls.
CVE-2017-6347	The ip_cmsg_recv_checksum function in net/ipv4/ip_sockglue.c in the Linux kernel before 4.10.1 has incorrect expectations about skb data layout, which allows local users to cause a denial of service (buffer over-read) or possibly have unspecified other impact via crafted system calls, as demonstrated by use of the MSG_MORE flag in conjunction with loopback UDP transmission.

CVE-2017-6348	The hashbin_delete function in net/irda/irqueue.c in the Linux kernel before 4.9.13 improperly manages lock dropping, which allows local users to cause a denial of service (deadlock) via crafted operations on IrDA devices.
CVE-2017-6362	Double free vulnerability in the gdImagePngPtr function in libgd2 before 2.2.5 allows remote attackers to cause a denial of service via vectors related to a palette with no colors.
CVE-2017-6418	libclamav/message.c in ClamAV 0.99.2 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted e-mail message.
CVE-2017-6419	mspack/lzxd.c in libmspack 0.5alpha, as used in ClamAV 0.99.2, allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted CHM file.
CVE-2017-6420	The wwunpack function in libclamav/wwunpack.c in ClamAV 0.99.2 allows remote attackers to cause a denial of service (use-after-free) via a crafted PE file with WWPack compression.
CVE-2017-6458	Multiple buffer overflows in the ctl_put* functions in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allow remote authenticated users to have unspecified impact via a long variable.
CVE-2017-6460	Stack-based buffer overflow in the reslist function in ntpq in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote servers have unspecified impact via a long flagstr variable in a restriction list response.
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-2017-6498	An issue was discovered in ImageMagick 6.9.7. Incorrect TGA files could trigger assertion failures, thus leading to DoS.
CVE-2017-6499	An issue was discovered in Magick++ in ImageMagick 6.9.7. A specially crafted file creating a nested exception could lead to a memory leak (thus, a DoS).

CVE-2017-6500	An issue was discovered in ImageMagick 6.9.7. A specially crafted sun file triggers a heap-based buffer over-read.
CVE-2017-6505	The ohci_service_ed_list function in hw/usb/hcd-ohci.c in QEMU (aka Quick Emulator) before 2.9.0 allows local guest OS users to cause a denial of service (infinite loop) via vectors involving the number of link endpoint list descriptors, a different vulnerability than CVE-2017-9330.
CVE-2017-6507	An issue was discovered in AppArmor before 2.12. Incorrect handling of unknown AppArmor profiles in AppArmor init scripts, upstart jobs, and/or systemd unit files allows an attacker to possibly have increased attack surfaces of processes that were intended to be confined by AppArmor. This is due to the common logic to handle 'restart' operations removing AppArmor profiles that aren't found in the typical filesystem locations, such as /etc/apparmor.d/. Userspace projects that manage their own AppArmor profiles in atypical directories, such as what's done by LXD and Docker, are affected by this flaw in the AppArmor init script logic.
CVE-2017-6508	CRLF injection vulnerability in the url_parse function in url.c in Wget through 1.19.1 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in the host subcomponent of a URL.
CVE-2017-6512	Race condition in the rmtree and remove_tree functions in the File-Path module before 2.13 for Perl allows attackers to set the mode on arbitrary files via vectors involving directory-permission loosening logic.
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-2017-6850	The jp2_cdef_destroy function in jp2_cod.c in JasPer before 2.0.13 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted image.
CVE-2017-6886	An error within the "parse_tiff_ifd()" function (internal/dcraw_common.cpp) in LibRaw versions before 0.18.2 can be exploited to corrupt memory.
CVE-2017-6887	A boundary error within the "parse_tiff_ifd()" function (internal/dcraw_common.cpp) in LibRaw versions before 0.18.2 can be exploited to cause a memory corruption via e.g. a specially crafted KDC file with

	model set to "DSLR-A100" and containing multiple sequences of 0x100 and 0x14A TAGs.
CVE-2017-6891	Two errors in the "asn1_find_node()" function (lib/parser_aux.c) within GnuTLS libtasn1 version 4.10 can be exploited to cause a stacked-based buffer overflow by tricking a user into processing a specially crafted assignments file via the e.g. asn1Coding utility.
CVE-2017-6964	dmcrypt-get-device, as shipped in the eject package of Debian and Ubuntu, does not check the return value of the (1) setuid or (2) setgid function, which might cause dmcrypt-get-device to execute code, which was intended to run as an unprivileged user, as root. This affects eject through 2.1.5+deb1+cvs20081104-13.1 on Debian, eject before 2.1.5+deb1+cvs20081104-13.1ubuntu0.16.10.1 on Ubuntu 16.10, eject before 2.1.5+deb1+cvs20081104-13.1ubuntu0.16.04.1 on Ubuntu 16.04 LTS, eject before 2.1.5+deb1+cvs20081104-13.1ubuntu0.14.04.1 on Ubuntu 14.04 LTS, and eject before 2.1.5+deb1+cvs20081104-9ubuntu0.1 on Ubuntu 12.04 LTS.
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-2017-7087	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7089	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. The issue involves the "WebKit" component. It allows remote attackers to conduct Universal XSS (UXSS) attacks via a crafted web site that is mishandled during parent-tab processing.
CVE-2017-7090	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to bypass the Same Origin Policy and obtain sensitive cookie information via a custom URL scheme.

CVE-2017-7091	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7092	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7093	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7095	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7096	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7098	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7100	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes

	before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7102	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7104	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7107	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7109	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. A cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script or HTML via crafted web content that incorrectly interacts with the Application Cache policy.
CVE-2017-7111	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7117	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component.

	It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7120	An issue was discovered in certain Apple products. iOS before 11 is affected. Safari before 11 is affected. iCloud before 7.0 on Windows is affected. iTunes before 12.7 on Windows is affected. tvOS before 11 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7153	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to spoof user-interface information (about whether the entire content is derived from a valid TLS session) via a crafted web site that sends a 401 Unauthorized redirect.
CVE-2017-7156	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7160	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2017-7161	An issue was discovered in certain Apple products. Safari before 11.0.2 is affected. The issue involves the "WebKit Web Inspector" component. It allows remote attackers to execute arbitrary code via special characters that trigger command injection.
CVE-2017-7165	An issue was discovered in certain Apple products. iOS before 11.2 is affected. Safari before 11.0.2 is affected. iCloud before 7.2 on Windows is affected. iTunes before 12.7.2 on Windows is affected. tvOS before 11.2 is affected. watchOS before 4.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2017-7184	The xfrm_replay_verify_len function in net/xfrm/xfrm_user.c in the Linux kernel through 4.10.6 does not validate certain size data after an XFRM_MSG_NEWAE update, which allows local users to obtain root privileges or cause a denial of service (heap-based out-of-bounds access) by leveraging the CAP_NET_ADMIN capability, as demonstrated during a Pwn2Own competition at CanSecWest 2017 for the Ubuntu 16.10 linux-image-* package 4.8.0.41.52.
CVE-2017-7187	The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel through 4.10.4 allows local users to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a large command size in an SG_NEXT_CMD_LEN ioctl call, leading to out-of-bounds write access in the sg_write function.
CVE-2017-7207	The mem_get_bits_rectangle function in Artifex Software, Inc. Ghostscript 9.20 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted PostScript document.
CVE-2017-7233	Django 1.10 before 1.10.7, 1.9 before 1.9.13, and 1.8 before 1.8.18 relies on user input in some cases to redirect the user to an "on success" URL. The security check for these redirects (namely ``django.utils.http.is_safe_url()``) considered some numeric URLs "safe" when they shouldn't be, aka an open redirect vulnerability. Also, if a developer relies on ``is_safe_url()`` to provide safe redirect targets and puts such a URL into a link, they could suffer from an XSS attack.
CVE-2017-7234	A maliciously crafted URL to a Django (1.10 before 1.10.7, 1.9 before 1.9.13, and 1.8 before 1.8.18) site using the ``django.views.static.serve()`` view could redirect to any other domain, aka an open redirect vulnerability.
CVE-2017-7261	The vmw_surface_define_ioctl function in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.10.5 does not check for a zero value of certain levels data, which allows local users to cause a denial of service (ZERO_SIZE_PTR dereference, and GPF and possibly panic) via a crafted ioctl call for a /dev/dri/renderD* device.
CVE-2017-7273	The cp_report_fixup function in drivers/hid/hid-cypress.c in the Linux kernel 4.x before 4.9.4 allows physically proximate attackers to cause a denial of service (integer underflow) or possibly have unspecified other impact via a crafted HID report.
CVE-2017-7294	The vmw_surface_define_ioctl function in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.10.6 does not validate addition of certain

	levels data, which allows local users to trigger an integer overflow and out-of-bounds write, and cause a denial of service (system hang or crash) or possibly gain privileges, via a crafted ioctl call for a /dev/dri/renderD* device.
CVE-2017-7308	The packet_set_ring function in net/packet/af_packet.c in the Linux kernel through 4.10.6 does not properly validate certain block-size data, which allows local users to cause a denial of service (integer signedness error and out-of-bounds write), or gain privileges (if the CAP_NET_RAW capability is held), via crafted system calls.
CVE-2017-7346	The vmw_gb_surface_define_ioctl function in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.10.7 does not validate certain levels data, which allows local users to cause a denial of service (system hang) via a crafted ioctl call for a /dev/dri/renderD* device.
CVE-2017-7358	In LightDM through 1.22.0, a directory traversal issue in debian/guest-account.sh allows local attackers to own arbitrary directory path locations and escalate privileges to root when the guest user logs out.
CVE-2017-7374	Use-after-free vulnerability in fs/crypto/ in the Linux kernel before 4.10.7 allows local users to cause a denial of service (NULL pointer dereference) or possibly gain privileges by revoking keyring keys being used for ext4, f2fs, or ubifs encryption, causing cryptographic transform objects to be freed prematurely.
CVE-2017-7375	A flaw in libxml2 allows remote XML entity inclusion with default parser flags (i.e., when the caller did not request entity substitution, DTD validation, external DTD subset loading, or default DTD attributes). Depending on the context, this may expose a higher-risk attack surface in libxml2 not usually reachable with default parser flags, and expose content from local files, HTTP, or FTP servers (which might be otherwise unreachable).
CVE-2017-7376	Buffer overflow in libxml2 allows remote attackers to execute arbitrary code by leveraging an incorrect limit for port values when handling redirects.
CVE-2017-7377	The (1) v9fs_create and (2) v9fs_lcreate functions in hw/9pfs/9p.c in QEMU (aka Quick Emulator) allow local guest OS privileged users to cause a denial of service (file descriptor or memory consumption) via vectors related to an already in-use fid.
CVE-2017-7407	The ourWriteOut function in tool_writeout.c in curl 7.53.1 might allow physically proximate attackers to obtain sensitive information from process memory in opportunistic circumstances by reading a workstation screen during use of a --write-out argument ending in a

	'%' character, which leads to a heap-based buffer over-read.
CVE-2017-7472	The KEYS subsystem in the Linux kernel before 4.10.13 allows local users to cause a denial of service (memory consumption) via a series of KEY_REQKEY_DEFL_THREAD_KEYRING keyctl_set_reqkey_keyring calls.
CVE-2017-7477	Heap-based buffer overflow in drivers/net/macsec.c in the MACsec module in the Linux kernel through 4.10.12 allows attackers to cause a denial of service or possibly have unspecified other impact by leveraging the use of a MAX_SKB_FRAGS+1 size in conjunction with the NETIF_F_FRAGLIST feature, leading to an error in the skb_to_sgvec function.
CVE-2017-7479	OpenVPN versions before 2.3.15 and before 2.4.2 are vulnerable to reachable assertion when packet-ID counter rolls over resulting into Denial of Service of server by authenticated attacker.
CVE-2017-7482	In the Linux kernel before version 4.12, Kerberos 5 tickets decoded when using the RXRPC keys incorrectly assumes the size of a field. This could lead to the size-remaining variable wrapping and the data pointer going over the end of the buffer. This could possibly lead to memory corruption and possible privilege escalation.
CVE-2017-7487	The ipxitf_ioctl function in net/ipx/af_ipx.c in the Linux kernel through 4.11.1 mishandles reference counts, which allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a failed SIOCGIFADDR ioctl call for an IPX interface.
CVE-2017-7493	Quick Emulator (Qemu) built with the VirtFS, host directory sharing via Plan 9 File System(9pfs) support, is vulnerable to an improper access control issue. It could occur while accessing virtfs metadata files in mapped-file security mode. A guest user could use this flaw to escalate their privileges inside guest.
CVE-2017-7494	Samba since version 3.5.0 and before 4.6.4, 4.5.10 and 4.4.14 is vulnerable to remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.
CVE-2017-7495	fs/ext4/inode.c in the Linux kernel before 4.6.2, when ext4 data=ordered mode is used, mishandles a needs-flushing-before-commit list, which allows local users to obtain sensitive information from other users' files in opportunistic circumstances by waiting for a hardware reset, creating a new file, making write system calls, and reading this file.

CVE-2017-7502	Null pointer dereference vulnerability in NSS since 3.24.0 was found when server receives empty SSLv2 messages resulting into denial of service by remote attacker.
CVE-2017-7506	spice versions though 0.13 are vulnerable to out-of-bounds memory access when processing specially crafted messages from authenticated attacker to the spice server resulting into crash and/or server memory leak.
CVE-2017-7507	GnuTLS version 3.5.12 and earlier is vulnerable to a NULL pointer dereference while decoding a status response TLS extension with valid contents. This could lead to a crash of the GnuTLS server application.
CVE-2017-7508	OpenVPN versions before 2.4.3 and before 2.3.17 are vulnerable to remote denial-of-service when receiving malformed IPv6 packet.
CVE-2017-7511	poppler since version 0.17.3 has been vulnerable to NULL pointer dereference in pdfunite triggered by specially crafted documents.
CVE-2017-7512	Red Hat 3scale (aka RH-3scale) API Management Platform (AMP) before 2.0.0 would permit creation of an access token without a client secret. An attacker could use this flaw to circumvent authentication controls and gain access to restricted APIs. NOTE: some sources have a typo in which CVE-2017-7512 maps to an OpenVPN vulnerability. The proper CVE ID for that OpenVPN vulnerability is CVE-2017-7521. Specifically, CVE-2017-7521 is the correct CVE ID for TWO closely related findings in OpenVPN. Any source that lists BOTH CVE-2017-7512 and CVE-2017-7521 for OpenVPN should have listed ONLY CVE-2017-7521.
CVE-2017-7515	poppler through version 0.55.0 is vulnerable to an uncontrolled recursion in pdfunite resulting into potential denial-of-service.
CVE-2017-7518	A flaw was found in the Linux kernel before version 4.12 in the way the KVM module processed the trap flag(TF) bit in EFLAGS during emulation of the syscall instruction, which leads to a debug exception(#DB) being raised in the guest stack. A user/process inside a guest could use this flaw to potentially escalate their privileges inside the guest. Linux guests are not affected by this.
CVE-2017-7520	OpenVPN versions before 2.4.3 and before 2.3.17 are vulnerable to denial-of-service and/or possibly sensitive memory leak triggered by man-in-the-middle attacker.
CVE-2017-7521	OpenVPN versions before 2.4.3 and before 2.3.17 are vulnerable to remote denial-of-service due to memory exhaustion caused by memory leaks and double-free issue in extract_x509_extension().

CVE-2017-7526	libgcrypt before version 1.7.8 is vulnerable to a cache side-channel attack resulting into a complete break of RSA-1024 while using the left-to-right method for computing the sliding-window expansion. The same attack is believed to work on RSA-2048 with moderately more computation. This side-channel requires that attacker can run arbitrary software on the hardware where the private RSA key is used.
CVE-2017-7529	Nginx versions since 0.5.6 up to and including 1.13.2 are vulnerable to integer overflow vulnerability in nginx range filter module resulting into leak of potentially sensitive information triggered by specially crafted request.
CVE-2017-7533	Race condition in the fsnotify implementation in the Linux kernel through 4.12.4 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that leverages simultaneous execution of the inotify_handle_event and vfs_rename functions.
CVE-2017-7541	The brcmf_cfg80211_mgmt_tx function in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c in the Linux kernel before 4.12.3 allows local users to cause a denial of service (buffer overflow and system crash) or possibly gain privileges via a crafted NL80211_CMD_FRAME Netlink packet.
CVE-2017-7546	PostgreSQL versions before 9.2.22, 9.3.18, 9.4.13, 9.5.8 and 9.6.4 are vulnerable to incorrect authentication flaw allowing remote attackers to gain access to database accounts with an empty password.
CVE-2017-7547	PostgreSQL versions before 9.2.22, 9.3.18, 9.4.13, 9.5.8 and 9.6.4 are vulnerable to authorization flaw allowing remote authenticated attackers to retrieve passwords from the user mappings defined by the foreign server owners without actually having the privileges to do so.
CVE-2017-7548	PostgreSQL versions before 9.4.13, 9.5.8 and 9.6.4 are vulnerable to authorization flaw allowing remote authenticated attackers with no privileges on a large object to overwrite the entire contents of the object, resulting in a denial of service.
CVE-2017-7555	Augeas versions up to and including 1.8.0 are vulnerable to heap-based buffer overflow due to improper handling of escaped strings. Attacker could send crafted strings that would cause the application using augeas to copy past the end of a buffer, leading to a crash or possible code execution.
CVE-2017-7585	In libsndfile before 1.0.28, an error in the "flac_buffer_copy()" function (flac.c) can be exploited to cause a stack-based buffer overflow via a specially crafted FLAC file.

CVE-2017-7586	In libsndfile before 1.0.28, an error in the "header_read()" function (common.c) when handling ID3 tags can be exploited to cause a stack-based buffer overflow via a specially crafted FLAC file.
CVE-2017-7592	The putagreytile function in tif_getimage.c in LibTIFF 4.0.7 has a left-shift undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.
CVE-2017-7593	tif_read.c in LibTIFF 4.0.7 does not ensure that tif_rawdata is properly initialized, which might allow remote attackers to obtain sensitive information from process memory via a crafted image.
CVE-2017-7594	The OJPEGReadHeaderInfoSecTablesDcTable function in tif_ojpeg.c in LibTIFF 4.0.7 allows remote attackers to cause a denial of service (memory leak) via a crafted image.
CVE-2017-7595	The JPEGSetupEncode function in tiff_jpeg.c in LibTIFF 4.0.7 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted image.
CVE-2017-7596	LibTIFF 4.0.7 has an "outside the range of representable values of type float" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.
CVE-2017-7597	tif_dirread.c in LibTIFF 4.0.7 has an "outside the range of representable values of type float" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.
CVE-2017-7598	tif_dirread.c in LibTIFF 4.0.7 might allow remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted image.
CVE-2017-7599	LibTIFF 4.0.7 has an "outside the range of representable values of type short" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.
CVE-2017-7600	LibTIFF 4.0.7 has an "outside the range of representable values of type unsigned char" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.
CVE-2017-7601	LibTIFF 4.0.7 has a "shift exponent too large for 64-bit type long" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.

CVE-2017-7602	LibTIFF 4.0.7 has a signed integer overflow, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.
CVE-2017-7606	coders/rle.c in ImageMagick 7.0.5-4 has an "outside the range of representable values of type unsigned char" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image.
CVE-2017-7607	The handle_gnu_hash function in readelf.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.
CVE-2017-7608	The ebl_object_note_type_name function in eblobjnotetypename.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.
CVE-2017-7609	elf_compress.c in elfutils 0.168 does not validate the zlib compression factor, which allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file.
CVE-2017-7610	The check_group function in elflint.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.
CVE-2017-7611	The check_symtab_shndx function in elflint.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.
CVE-2017-7612	The check_sysv_hash function in elflint.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.
CVE-2017-7613	elflint.c in elfutils 0.168 does not validate the number of sections and the number of segments, which allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file.
CVE-2017-7616	Incorrect error handling in the set_mempolicy and mbind compat syscalls in mm/mempolicy.c in the Linux kernel through 4.10.9 allows local users to obtain sensitive information from uninitialized stack data by triggering failure of a certain bitmap operation.
CVE-2017-7618	crypto/ahash.c in the Linux kernel through 4.10.9 allows attackers to cause a denial of service (API operation calling its own callback, and infinite recursion) by triggering EBUSY on a full queue.

CVE-2017-7619	In ImageMagick 7.0.4-9, an infinite loop can occur because of a floating-point rounding error in some of the color algorithms. This affects ModulateHSL, ModulateHCL, ModulateHCLp, ModulateHSB, ModulateHSI, ModulateHSV, ModulateHWB, ModulateLCHab, and ModulateLCHuv.
CVE-2017-7645	The NFSv2/NFSv3 server in the nfsd subsystem in the Linux kernel through 4.10.11 allows remote attackers to cause a denial of service (system crash) via a long RPC reply, related to net/sunrpc/svc.c, fs/nfsd/nfs3xdr.c, and fs/nfsd/nfsxdr.c.
CVE-2017-7668	The HTTP strict parsing changes added in Apache httpd 2.2.32 and 2.4.24 introduced a bug in token list parsing, which allows ap_find_token() to search past the end of its input string. By maliciously crafting a sequence of request headers, an attacker may be able to cause a segmentation fault, or to force ap_find_token() to return an incorrect value.
CVE-2017-7674	The CORS Filter in Apache Tomcat 9.0.0.M1 to 9.0.0.M21, 8.5.0 to 8.5.15, 8.0.0.RC1 to 8.0.44 and 7.0.41 to 7.0.78 did not add an HTTP Vary header indicating that the response varies depending on Origin. This permitted client and server side cache poisoning in some circumstances.
CVE-2017-7679	In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_mime can read one byte past the end of a buffer when sending a malicious Content-Type response header.
CVE-2017-7718	hw/display/cirrus_vga_rop.h in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (out-of-bounds read and QEMU process crash) via vectors related to copying VGA data via the cirrus_bitblt_rop_fwd_transp_ and cirrus_bitblt_rop_fwd_ functions.
CVE-2017-7741	In libsndfile before 1.0.28, an error in the "flac_buffer_copy()" function (flac.c) can be exploited to cause a segmentation violation (with write memory access) via a specially crafted FLAC file during a resample attempt, a similar issue to CVE-2017-7585.
CVE-2017-7742	In libsndfile before 1.0.28, an error in the "flac_buffer_copy()" function (flac.c) can be exploited to cause a segmentation violation (with read memory access) via a specially crafted FLAC file during a resample attempt, a similar issue to CVE-2017-7585.
CVE-2017-7749	A use-after-free vulnerability when using an incorrect URL during the reloading of a docshell. This results in a potentially exploitable crash. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.

CVE-2017-7750	A use-after-free vulnerability during video control operations when a "<track>" element holds a reference to an older window if that window has been replaced in the DOM. This results in a potentially exploitable crash. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7751	A use-after-free vulnerability with content viewer listeners that results in a potentially exploitable crash. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7752	A use-after-free vulnerability during specific user interactions with the input method editor (IME) in some languages due to how events are handled. This results in a potentially exploitable crash but would require specific user interaction to trigger. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7753	An out-of-bounds read occurs when applying style rules to pseudo-elements, such as ::first-line, using cached style data. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
CVE-2017-7754	An out-of-bounds read in WebGL with a maliciously crafted "ImageInfo" object during WebGL operations. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7756	A use-after-free and use-after-scope vulnerability when logging errors from headers for XML HTTP Requests (XHR). This could result in a potentially exploitable crash. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7757	A use-after-free vulnerability in IndexedDB when one of its objects is destroyed in memory while a method on it is still being executed. This results in a potentially exploitable crash. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7758	An out-of-bounds read vulnerability with the Opus encoder when the number of channels in an audio stream changes while the encoder is in use. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7762	When entered directly, Reader Mode did not strip the username and password section of URLs displayed in the addressbar. This can be used for spoofing the domain of the current page. This vulnerability affects Firefox < 54.
CVE-2017-7764	Characters from the "Canadian Syllabics" unicode block can be mixed with characters from other unicode blocks in the addressbar instead of being rendered as their raw "punycode" form, allowing for domain name spoofing attacks through character confusion. The current

	Unicode standard allows characters from "Aspirational Use Scripts" such as Canadian Syllabics to be mixed with Latin characters in the "moderately restrictive" IDN profile. We have changed Firefox behavior to match the upcoming Unicode version 10.0 which removes this category and treats them as "Limited Use Scripts.". This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7771	An out of bounds read flaw related to "graphite2::Pass::readPass" has been reported in graphite2. An attacker could possibly exploit this flaw to disclose potentially sensitive memory or cause an application crash.
CVE-2017-7772	A heap-based buffer overflow flaw related to "lz4::decompress" has been reported in graphite2. An attacker could exploit this issue to cause a crash or, possibly, execute arbitrary code.
CVE-2017-7773	A heap-based buffer overflow flaw related to "lz4::decompress" (src/Decompressor) has been reported in graphite2. An attacker could exploit this issue to cause a crash or, possibly, execute arbitrary code.
CVE-2017-7774	An out of bounds read flaw related to "graphite2::Silf::readGraphite" has been reported in graphite2. An attacker could possibly exploit this flaw to disclose potentially sensitive memory or cause an application crash.
CVE-2017-7775	An assertion error has been reported in graphite2. An attacker could possibly exploit this flaw to cause an application crash.
CVE-2017-7776	An out of bounds read flaw related to "graphite2::Silf::getClassGlyph" has been reported in graphite2. An attacker could possibly exploit this flaw to disclose potentially sensitive memory or cause an application crash.
CVE-2017-7777	The use of uninitialized memory related to "graphite2::GlyphCache::Loader::read_glyph" has been reported in graphite2. An attacker could possibly exploit this flaw to negatively impact the execution of an application using graphite2 in unknown ways.
CVE-2017-7778	A number of security vulnerabilities in the Graphite 2 library including out-of-bounds reads, buffer overflow reads and writes, and the use of uninitialized memory. These issues were addressed in Graphite 2 version 1.3.10. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7779	Memory safety bugs were reported in Firefox 54, Firefox ESR 52.2, and Thunderbird 52.2. 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 Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
CVE-2017-7780	Memory safety bugs were reported in Firefox 54. 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 < 55.
CVE-2017-7781	An error occurs in the elliptic curve point addition algorithm that uses mixed Jacobian-affine coordinates where it can yield a result "POINT_AT_INFINITY" when it should not. A man-in-the-middle attacker could use this to interfere with a connection, resulting in an attacked party computing an incorrect shared secret. This vulnerability affects Firefox < 55.
CVE-2017-7783	If a long user name is used in a username/ password combination in a site URL (such as " http://UserName:Password@example.com"), the resulting modal prompt will hang in a non-responsive state or crash, causing a denial of service. This vulnerability affects Firefox < 55.
CVE-2017-7784	A use-after-free vulnerability can occur when reading an image observer during frame reconstruction after the observer has been freed. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
CVE-2017-7785	A buffer overflow can occur when manipulating Accessible Rich Internet Applications (ARIA) attributes within the DOM. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
CVE-2017-7786	A buffer overflow can occur when the image renderer attempts to paint non-displayable SVG elements. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
CVE-2017-7787	Same-origin policy protections can be bypassed on pages with embedded iframes during page reloads, allowing the iframes to access content on the top level page, leading to information disclosure. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
CVE-2017-7788	When an "iframe" has a "sandbox" attribute and its content is specified using "srcdoc", that content does not inherit the containing page's Content Security Policy (CSP) as it should unless the sandbox attribute included "allow-same-origin". This vulnerability affects Firefox < 55.
CVE-2017-7789	If a server sends two Strict-Transport-Security (STS) headers for a single connection, they will be rejected

	as invalid and HTTP Strict Transport Security (HSTS) will not be enabled for the connection. This vulnerability affects Firefox < 55.
CVE-2017-7791	On pages containing an iframe, the "data:" protocol can be used to create a modal alert that will render over arbitrary domains following page navigation, spoofing of the origin of the modal alert from the iframe content. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
CVE-2017-7792	A buffer overflow will occur when viewing a certificate in the certificate manager if the certificate has an extremely long object identifier (OID). This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
CVE-2017-7793	A use-after-free vulnerability can occur in the Fetch API when the worker or the associated window are freed when still in use, resulting in a potentially exploitable crash. This vulnerability affects Firefox < 56, Firefox ESR < 52.4, and Thunderbird < 52.4.
CVE-2017-7794	On Linux systems, if the content process is compromised, the sandbox broker will allow files to be truncated even though the sandbox explicitly only has read access to the local file system and no write permissions. Note: This attack only affects the Linux operating system. Other operating systems are not affected. This vulnerability affects Firefox < 55.
CVE-2017-7797	Response header name interning does not have same-origin protections and these headers are stored in a global registry. This allows stored header names to be available cross-origin. This vulnerability affects Firefox < 55.
CVE-2017-7798	The Developer Tools feature suffers from a XUL injection vulnerability due to improper sanitization of the web page source code. In the worst case, this could allow arbitrary code execution when opening a malicious page with the style editor tool. This vulnerability affects Firefox ESR < 52.3 and Firefox < 55.
CVE-2017-7799	JavaScript in the "about:webrtc" page is not sanitized properly being assigned to "innerHTML". Data on this page is supplied by WebRTC usage and is not under third-party control, making this difficult to exploit, but the vulnerability could possibly be used for a cross-site scripting (XSS) attack. This vulnerability affects Firefox < 55.
CVE-2017-7800	A use-after-free vulnerability can occur in WebSockets when the object holding the connection is freed before the disconnection operation is finished. This results in an exploitable crash. This vulnerability affects

	Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
CVE-2017-7801	A use-after-free vulnerability can occur while re-computing layout for a "marquee" element during window resizing where the updated style object is freed while still in use. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
CVE-2017-7802	A use-after-free vulnerability can occur when manipulating the DOM during the resize event of an image element. If these elements have been freed due to a lack of strong references, a potentially exploitable crash may occur when the freed elements are accessed. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
CVE-2017-7803	When a page's content security policy (CSP) header contains a "sandbox" directive, other directives are ignored. This results in the incorrect enforcement of CSP. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
CVE-2017-7805	During TLS 1.2 exchanges, handshake hashes are generated which point to a message buffer. This saved data is used for later messages but in some cases, the handshake transcript can exceed the space available in the current buffer, causing the allocation of a new buffer. This leaves a pointer pointing to the old, freed buffer, resulting in a use-after-free when handshake hashes are then calculated afterwards. This can result in a potentially exploitable crash. This vulnerability affects Firefox < 56, Firefox ESR < 52.4, and Thunderbird < 52.4.
CVE-2017-7806	A use-after-free vulnerability can occur when the layer manager is freed too early when rendering specific SVG content, resulting in a potentially exploitable crash. This vulnerability affects Firefox < 55.
CVE-2017-7807	A mechanism that uses AppCache to hijack a URL in a domain using fallback by serving the files from a sub-path on the domain. This has been addressed by requiring fallback files be inside the manifest directory. This vulnerability affects Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
CVE-2017-7808	A content security policy (CSP) "frame-ancestors" directive containing origins with paths allows for comparisons against those paths instead of the origin. This results in a cross-origin information leak of this path information. This vulnerability affects Firefox < 55.
CVE-2017-7809	A use-after-free vulnerability can occur when an editor DOM node is deleted prematurely during tree traversal while still bound to the document. This results in a potentially exploitable crash. This vulnerability affects

	Thunderbird < 52.3, Firefox ESR < 52.3, and Firefox < 55.
CVE-2017-7810	Memory safety bugs were reported in Firefox 55 and Firefox ESR 52.3. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 56, Firefox ESR < 52.4, and Thunderbird < 52.4.
CVE-2017-7811	Memory safety bugs were reported in Firefox 55. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 56.
CVE-2017-7812	If web content on a page is dragged onto portions of the browser UI, such as the tab bar, links can be opened that otherwise would not be allowed to open. This can allow malicious web content to open a locally stored file through "file:" URLs. This vulnerability affects Firefox < 56.
CVE-2017-7813	Inside the JavaScript parser, a cast of an integer to a narrower type can result in data read from outside the buffer being parsed. This usually results in a non-exploitable crash, but can leak a limited amount of information from memory if it matches JavaScript identifier syntax. This vulnerability affects Firefox < 56.
CVE-2017-7814	File downloads encoded with "blob:" and "data:" URL elements bypassed normal file download checks though the Phishing and Malware Protection feature and its block lists of suspicious sites and files. This would allow malicious sites to lure users into downloading executables that would otherwise be detected as suspicious. This vulnerability affects Firefox < 56, Firefox ESR < 52.4, and Thunderbird < 52.4.
CVE-2017-7815	On pages containing an iframe, the "data:" protocol can be used to create a modal dialog through Javascript that will have an arbitrary domains as the dialog's location, spoofing of the origin of the modal dialog from the user view. Note: This attack only affects installations with e10 multiprocess turned off. Installations with e10s turned on do not support the modal dialog functionality. This vulnerability affects Firefox < 56.
CVE-2017-7816	WebExtensions could use popups and panels in the extension UI to load an "about:" privileged URL, violating security checks that disallow this behavior. This vulnerability affects Firefox < 56.
CVE-2017-7818	A use-after-free vulnerability can occur when manipulating arrays of Accessible Rich Internet Applications (ARIA) elements within containers through the DOM. This results in a potentially exploitable crash.

	This vulnerability affects Firefox < 56, Firefox ESR < 52.4, and Thunderbird < 52.4.
CVE-2017-7819	A use-after-free vulnerability can occur in design mode when image objects are resized if objects referenced during the resizing have been freed from memory. This results in a potentially exploitable crash. This vulnerability affects Firefox < 56, Firefox ESR < 52.4, and Thunderbird < 52.4.
CVE-2017-7820	The "instanceof" operator can bypass the Xray wrapper mechanism. When called on web content from the browser itself or an extension the web content can provide its own result for that operator, possibly tricking the browser or extension into mishandling the element. This vulnerability affects Firefox < 56.
CVE-2017-7821	A vulnerability where WebExtensions can download and attempt to open a file of some non-executable file types. This can be triggered without specific user interaction for the file download and open actions. This could be used to trigger known vulnerabilities in the programs that handle those document types. This vulnerability affects Firefox < 56.
CVE-2017-7822	The AES-GCM implementation in WebCrypto API accepts 0-length IV when it should require a length of 1 according to the NIST Special Publication 800-38D specification. This might allow for the authentication key to be determined in some instances. This vulnerability affects Firefox < 56.
CVE-2017-7823	The content security policy (CSP) "sandbox" directive did not create a unique origin for the document, causing it to behave as if the "allow-same-origin" keyword were always specified. This could allow a Cross-Site Scripting (XSS) attack to be launched from unsafe content. This vulnerability affects Firefox < 56, Firefox ESR < 52.4, and Thunderbird < 52.4.
CVE-2017-7824	A buffer overflow occurs when drawing and validating elements with the ANGLE graphics library, used for WebGL content. This is due to an incorrect value being passed within the library during checks and results in a potentially exploitable crash. This vulnerability affects Firefox < 56, Firefox ESR < 52.4, and Thunderbird < 52.4.
CVE-2017-7826	Memory safety bugs were reported in Firefox 56 and Firefox ESR 52.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 57, Firefox ESR < 52.5, and Thunderbird < 52.5.
CVE-2017-7827	Memory safety bugs were reported in Firefox 56. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of

	these could be exploited to run arbitrary code. This vulnerability affects Firefox < 57.
CVE-2017-7828	A use-after-free vulnerability can occur when flushing and resizing layout because the "PressShell" object has been freed while still in use. This results in a potentially exploitable crash during these operations. This vulnerability affects Firefox < 57, Firefox ESR < 52.5, and Thunderbird < 52.5.
CVE-2017-7829	It is possible to spoof the sender's email address and display an arbitrary sender address to the email recipient. The real sender's address is not displayed if preceded by a null character in the display string. This vulnerability affects Thunderbird < 52.5.2.
CVE-2017-7830	The Resource Timing API incorrectly revealed navigations in cross-origin iframes. This is a same-origin policy violation and could allow for data theft of URLs loaded by users. This vulnerability affects Firefox < 57, Firefox ESR < 52.5, and Thunderbird < 52.5.
CVE-2017-7831	A vulnerability where the security wrapper does not deny access to some exposed properties using the deprecated "_exposedProps_" mechanism on proxy objects. These properties should be explicitly unavailable to proxy objects. This vulnerability affects Firefox < 57.
CVE-2017-7832	The combined, single character, version of the letter 'i' with any of the potential accents in unicode, such as acute or grave, can be spoofed in the addressbar by the dotless version of 'i' followed by the same accent as a second character with most font sets. This allows for domain spoofing attacks because these combined domain names do not display as punycode. This vulnerability affects Firefox < 57.
CVE-2017-7833	Some Arabic and Indic vowel marker characters can be combined with Latin characters in a domain name to eclipse the non-Latin character with some font sets on the addressbar. The non-Latin character will not be visible to most viewers. This allows for domain spoofing attacks because these combined domain names do not display as punycode. This vulnerability affects Firefox < 57.
CVE-2017-7834	A "data:" URL loaded in a new tab did not inherit the Content Security Policy (CSP) of the original page, allowing for bypasses of the policy including the execution of JavaScript. In prior versions when "data:" documents also inherited the context of the original page this would allow for potential cross-site scripting (XSS) attacks. This vulnerability affects Firefox < 57.
CVE-2017-7835	Mixed content blocking of insecure (HTTP) sub-resources in a secure (HTTPS) document was not correctly applied for resources that redirect from HTTPS

	to HTTP, allowing content that should be blocked, such as scripts, to be loaded on a page. This vulnerability affects Firefox < 57.
CVE-2017-7837	SVG loaded through "<img>" tags can use "<meta>" tags within the SVG data to set cookies for that page. This vulnerability affects Firefox < 57.
CVE-2017-7838	Punycode format text will be displayed for entire qualified international domain names in some instances when a sub-domain triggers the punycode display instead of the primary domain being displayed in native script and the sub-domain only displaying as punycode. This could be used for limited spoofing attacks due to user confusion. This vulnerability affects Firefox < 57.
CVE-2017-7839	Control characters prepended before "javascript:" URLs pasted in the addressbar can cause the leading characters to be ignored and the pasted JavaScript to be executed instead of being blocked. This could be used in social engineering and self-cross-site-scripting (self-XSS) attacks where users are convinced to copy and paste text into the addressbar. This vulnerability affects Firefox < 57.
CVE-2017-7840	JavaScript can be injected into an exported bookmarks file by placing JavaScript code into user-supplied tags in saved bookmarks. If the resulting exported HTML file is later opened in a browser this JavaScript will be executed. This could be used in social engineering and self-cross-site-scripting (self-XSS) attacks if users were convinced to add malicious tags to bookmarks, export them, and then open the resulting file. This vulnerability affects Firefox < 57.
CVE-2017-7842	If a document's Referrer Policy attribute is set to "no-referrer" sometimes two network requests are made for "<link>" elements instead of one. One of these requests includes the referrer instead of respecting the set policy to not include a referrer on requests. This vulnerability affects Firefox < 57.
CVE-2017-7846	It is possible to execute JavaScript in the parsed RSS feed when RSS feed is viewed as a website, e.g. via "View -> Feed article -> Website" or in the standard format of "View -> Feed article -> default format". This vulnerability affects Thunderbird < 52.5.2.
CVE-2017-7847	Crafted CSS in an RSS feed can leak and reveal local path strings, which may contain user name. This vulnerability affects Thunderbird < 52.5.2.
CVE-2017-7848	RSS fields can inject new lines into the created email structure, modifying the message body. This vulnerability affects Thunderbird < 52.5.2.
CVE-2017-7867	International Components for Unicode (ICU) for C/C++ before 2017-02-13 has an out-of-bounds write caused by a heap-based buffer overflow related to the

	utf8TextAccess function in common/utext.cpp and the utext_setNativeIndex* function.
CVE-2017-7868	International Components for Unicode (ICU) for C/C++ before 2017-02-13 has an out-of-bounds write caused by a heap-based buffer overflow related to the utf8TextAccess function in common/utext.cpp and the utext_moveIndex32* function.
CVE-2017-7869	GnuTLS before 2017-02-20 has an out-of-bounds write caused by an integer overflow and heap-based buffer overflow related to the cdk_pkt_read function in opencdk/read-packet.c. This issue (which is a subset of the vendor's GNUTLS-SA-2017-3 report) is fixed in 3.5.10.
CVE-2017-7870	LibreOffice before 2017-01-02 has an out-of-bounds write caused by a heap-based buffer overflow related to the tools::Polygon::Insert function in tools/source/generic/poly.cxx.
CVE-2017-7885	Artifex jbig2dec 0.13 has a heap-based buffer over-read leading to denial of service (application crash) or disclosure of sensitive information from process memory, because of an integer overflow in the jbig2_decode_symbol_dict function in jbig2_symbol_dict.c in libjbig2dec.a during operation on a crafted .jb2 file.
CVE-2017-7889	The mm subsystem in the Linux kernel through 4.10.10 does not properly enforce the CONFIG_STRICT_DEVMEM protection mechanism, which allows local users to read or write to kernel memory locations in the first megabyte (and bypass slab-allocation access restrictions) via an application that opens the /dev/mem file, related to arch/x86/mm/init.c and drivers/char/mem.c.
CVE-2017-7890	The GIF decoding function gdImageCreateFromGifCtx in gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.31 and 7.x before 7.1.7, does not zero colorMap arrays before use. A specially crafted GIF image could use the uninitialized tables to read ~700 bytes from the top of the stack, potentially disclosing sensitive information.
CVE-2017-7895	The NFSv2 and NFSv3 server implementations in the Linux kernel through 4.10.13 lack certain checks for the end of a buffer, which allows remote attackers to trigger pointer-arithmetic errors or possibly have unspecified other impact via crafted requests, related to fs/nfsd/nfs3xdr.c and fs/nfsd/nfsxdr.c.
CVE-2017-7941	The ReadSGIImage function in sgi.c in ImageMagick 7.0.5-4 allows remote attackers to consume an amount of available memory via a crafted file.

CVE-2017-7942	The ReadAVSImage function in avs.c in ImageMagick 7.0.5-4 allows remote attackers to consume an amount of available memory via a crafted file.
CVE-2017-7943	The ReadSVGImage function in svg.c in ImageMagick 7.0.5-4 allows remote attackers to consume an amount of available memory via a crafted file.
CVE-2017-7975	Artifex jbig2dec 0.13, as used in Ghostscript, allows out-of-bounds writes because of an integer overflow in the jbig2_build_huffman_table function in jbig2_huffman.c during operations on a crafted JBIG2 file, leading to a denial of service (application crash) or possibly execution of arbitrary code.
CVE-2017-7976	Artifex jbig2dec 0.13 allows out-of-bounds writes and reads because of an integer overflow in the jbig2_image_compose function in jbig2_image.c during operations on a crafted .jb2 file, leading to a denial of service (application crash) or disclosure of sensitive information from process memory.
CVE-2017-7980	Heap-based buffer overflow in Cirrus CLGD 54xx VGA Emulator in Quick Emulator (Qemu) 2.8 and earlier allows local guest OS users to execute arbitrary code or cause a denial of service (crash) via vectors related to a VNC client updating its display after a VGA operation.
CVE-2017-7982	Integer overflow in the plist_from_bin function in bplist.c in libimobiledevice/libplist before 2017-04-19 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted plist file.
CVE-2017-8086	Memory leak in the v9fs_list_xattr function in hw/9pfs/9p-xattr.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (memory consumption) via vectors involving the orig_value variable.
CVE-2017-8105	FreeType 2 before 2017-03-24 has an out-of-bounds write caused by a heap-based buffer overflow related to the t1_decoder_parse_charstrings function in psaux/t1decode.c.
CVE-2017-8112	hw/scsi/vmw_pvscsi.c in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (infinite loop and CPU consumption) via the message ring page count.
CVE-2017-8287	FreeType 2 before 2017-03-26 has an out-of-bounds write caused by a heap-based buffer overflow related to the t1_builder_close_contour function in psaux/psobjs.c.
CVE-2017-8291	Artifex Ghostscript through 2017-04-26 allows -dSAFER bypass and remote command execution via .rsdparams type confusion with a "/OutputFile (%pipe%" substring

	in a crafted .eps document that is an input to the gs program, as exploited in the wild in April 2017.
CVE-2017-8309	Memory leak in the audio/audio.c in QEMU (aka Quick Emulator) allows remote attackers to cause a denial of service (memory consumption) by repeatedly starting and stopping audio capture.
CVE-2017-8343	In ImageMagick 7.0.5-5, the ReadAAIImage function in aai.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-8344	In ImageMagick 7.0.5-5, the ReadPCXImage function in pcx.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-8345	In ImageMagick 7.0.5-5, the ReadMNGImage function in png.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-8346	In ImageMagick 7.0.5-5, the ReadDCMImage function in dcm.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-8347	In ImageMagick 7.0.5-5, the ReadEXRImage function in exr.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-8348	In ImageMagick 7.0.5-5, the ReadMATImage function in mat.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-8349	In ImageMagick 7.0.5-5, the ReadSFWImage function in sfw.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-8350	In ImageMagick 7.0.5-5, the ReadJNGImage function in png.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-8351	In ImageMagick 7.0.5-5, the ReadPCDImage function in pcd.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-8352	In ImageMagick 7.0.5-5, the ReadXWDImage function in xwd.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-8353	In ImageMagick 7.0.5-5, the ReadPICTImage function in pict.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-8354	In ImageMagick 7.0.5-5, the ReadBMPImage function in bmp.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-8355	In ImageMagick 7.0.5-5, the ReadMTVImage function in mtv.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-8356	In ImageMagick 7.0.5-5, the ReadSUNImage function in sun.c allows attackers to cause a denial of service (memory leak) via a crafted file.

CVE-2017-8357	In ImageMagick 7.0.5-5, the ReadEPTImage function in ept.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-8361	The flac_buffer_copy function in flac.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (buffer overflow and application crash) or possibly have unspecified other impact via a crafted audio file.
CVE-2017-8362	The flac_buffer_copy function in flac.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (invalid read and application crash) via a crafted audio file.
CVE-2017-8363	The flac_buffer_copy function in flac.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted audio file.
CVE-2017-8365	The i2les_array function in pcm.c in libsndfile 1.0.28 allows remote attackers to cause a denial of service (buffer over-read and application crash) via a crafted audio file.
CVE-2017-8379	Memory leak in the keyboard input event handlers support in QEMU (aka Quick Emulator) allows local guest OS privileged users to cause a denial of service (host memory consumption) by rapidly generating large keyboard events.
CVE-2017-8380	Buffer overflow in the "megasas_mmio_write" function in Qemu 2.9.0 allows remote attackers to have unspecified impact via unknown vectors.
CVE-2017-8386	git-shell in git before 2.4.12, 2.5.x before 2.5.6, 2.6.x before 2.6.7, 2.7.x before 2.7.5, 2.8.x before 2.8.5, 2.9.x before 2.9.4, 2.10.x before 2.10.3, 2.11.x before 2.11.2, and 2.12.x before 2.12.3 might allow remote authenticated users to gain privileges via a repository name that starts with a - (dash) character.
CVE-2017-8765	The function named ReadICONImage in coders\icon.c in ImageMagick 7.0.5-5 has a memory leak vulnerability which can cause memory exhaustion via a crafted ICON file.
CVE-2017-8779	rpcbind through 0.2.4, LIBTIRPC through 1.0.1 and 1.0.2-rc through 1.0.2-rc3, and NTIRPC through 1.4.3 do not consider the maximum RPC data size during memory allocation for XDR strings, which allows remote attackers to cause a denial of service (memory consumption with no subsequent free) via a crafted UDP packet to port 111, aka rpcbomb.
CVE-2017-8798	Integer signedness error in MiniUPnP MiniUPnPc v1.4.20101221 through v2.0 allows remote attackers to cause a denial of service or possibly have unspecified other impact.

CVE-2017-8806	The Debian pg_ctlcluster, pg_createcluster, and pg_upgradecluster scripts, as distributed in the Debian postgresql-common package before 181+deb9u1 for PostgreSQL (and other packages related to Debian and Ubuntu), handled symbolic links insecurely, which could result in local denial of service by overwriting arbitrary files.
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-2017-8824	The dccp_disconnect function in net/dccp/proto.c in the Linux kernel through 4.14.3 allows local users to gain privileges or cause a denial of service (use-after-free) via an AF_UNSPEC connect system call during the DCCP_LISTEN state.
CVE-2017-8829	Deserialization vulnerability in lintian through 2.5.50.3 allows attackers to trigger code execution by requesting a review of a source package with a crafted YAML file.
CVE-2017-8830	In ImageMagick 7.0.5-6, the ReadBMPImage function in bmp.c:1379 allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-8831	The saa7164_bus_get function in drivers/media/pci/saa7164/saa7164-bus.c in the Linux kernel through 4.11.5 allows local users to cause a denial of service (out-of-bounds array access) or possibly have unspecified other impact by changing a certain sequence-number value, aka a "double fetch" vulnerability.
CVE-2017-8890	The inet_csk_clone_lock function in net/ipv4/inet_connection_sock.c in the Linux kernel through 4.10.15 allows attackers to cause a denial of service (double free) or possibly have unspecified other impact by leveraging use of the accept system call.
CVE-2017-8924	The edge_bulk_in_callback function in drivers/usb/serial/io_ti.c in the Linux kernel before 4.10.4 allows local users to obtain sensitive information (in the dmesg ringbuffer and syslog) from uninitialized kernel memory by using a crafted USB device (posing as an io_ti USB serial device) to trigger an integer underflow.
CVE-2017-8925	The omninet_open function in drivers/usb/serial/omninet.c in the Linux kernel before 4.10.4 allows local

	users to cause a denial of service (tty exhaustion) by leveraging reference count mishandling.
CVE-2017-9022	The gmp plugin in strongSwan before 5.5.3 does not properly validate RSA public keys before calling mpz_powm_sec, which allows remote peers to cause a denial of service (floating point exception and process crash) via a crafted certificate.
CVE-2017-9023	The ASN.1 parser in strongSwan before 5.5.3 improperly handles CHOICE types when the x509 plugin is enabled, which allows remote attackers to cause a denial of service (infinite loop) via a crafted certificate.
CVE-2017-9047	A buffer overflow was discovered in libxml2 20904-GITv2.9.4-16-g0741801. The function xmlSnprintfElementContent in valid.c is supposed to recursively dump the element content definition into a char buffer 'buf' of size 'size'. The variable len is assigned strlen(buf). If the content->type is XML_ELEMENT_CONTENT_ELEMENT, then (i) the content->prefix is appended to buf (if it actually fits) whereupon (ii) content->name is written to the buffer. However, the check for whether the content->name actually fits also uses 'len' rather than the updated buffer length strlen(buf). This allows us to write about "size" many bytes beyond the allocated memory. This vulnerability causes programs that use libxml2, such as PHP, to crash.
CVE-2017-9048	libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a stack-based buffer overflow. The function xmlSnprintfElementContent in valid.c is supposed to recursively dump the element content definition into a char buffer 'buf' of size 'size'. At the end of the routine, the function may strcat two more characters without checking whether the current strlen(buf) + 2 < size. This vulnerability causes programs that use libxml2, such as PHP, to crash.
CVE-2017-9049	libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a heap-based buffer over-read in the xmlDictComputeFastKey function in dict.c. This vulnerability causes programs that use libxml2, such as PHP, to crash. This vulnerability exists because of an incomplete fix for libxml2 Bug 759398.
CVE-2017-9050	libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a heap-based buffer over-read in the xmlDictAddString function in dict.c. This vulnerability causes programs that use libxml2, such as PHP, to crash. This vulnerability exists because of an incomplete fix for CVE-2016-1839.
CVE-2017-9060	Memory leak in the virtio_gpu_set_scanout function in hw/display/virtio-gpu.c in QEMU (aka Quick Emulator) allows local guest OS users to cause a denial of

	service (memory consumption) via a large number of "VIRTIO_GPU_CMD_SET_SCANOUT:" commands.
CVE-2017-9074	The IPv6 fragmentation implementation in the Linux kernel through 4.11.1 does not consider that the nexthdr field may be associated with an invalid option, which allows local users to cause a denial of service (out-of-bounds read and BUG) or possibly have unspecified other impact via crafted socket and send system calls.
CVE-2017-9075	The sctp_v6_create_accept_sk function in net/sctp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.
CVE-2017-9076	The dccp_v6_request_recv_sock function in net/dccp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.
CVE-2017-9077	The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.
CVE-2017-9083	poppler 0.54.0, as used in Evince and other products, has a NULL pointer dereference in the JPXStream::readUByte function in JPXStream.cc. For example, the perf_test utility will crash (segmentation fault) when parsing an invalid PDF file.
CVE-2017-9098	ImageMagick before 7.0.5-2 and GraphicsMagick before 1.3.24 use uninitialized memory in the RLE decoder, allowing an attacker to leak sensitive information from process memory space, as demonstrated by remote attacks against ImageMagick code in a long-running server process that converts image data on behalf of multiple users. This is caused by a missing initialization step in the ReadRLEImage function in coders/rle.c.
CVE-2017-9117	In LibTIFF 4.0.7, the program processes BMP images without verifying that biWidth and biHeight in the bitmap-information header match the actual input, leading to a heap-based buffer over-read in bmp2tiff.
CVE-2017-9141	In ImageMagick 7.0.5-7 Q16, a crafted file could trigger an assertion failure in the ResetImageProfileIterator function in MagickCore/profile.c because of missing checks in the ReadDDSImage function in coders/dds.c.
CVE-2017-9142	In ImageMagick 7.0.5-7 Q16, a crafted file could trigger an assertion failure in the WriteBlob function in

	MagickCore/blob.c because of missing checks in the ReadOneJNGImage function in coders/png.c.
CVE-2017-9143	In ImageMagick 7.0.5-5, the ReadARTImage function in coders/art.c allows attackers to cause a denial of service (memory leak) via a crafted .art file.
CVE-2017-9144	In ImageMagick 7.0.5-5, a crafted RLE image can trigger a crash because of incorrect EOF handling in coders/rle.c.
CVE-2017-9147	LibTIFF 4.0.7 has an invalid read in the _TIFFVGetField function in tif_dir.c, which might allow remote attackers to cause a denial of service (crash) via a crafted TIFF file.
CVE-2017-9150	The do_check function in kernel/bpf/verifier.c in the Linux kernel before 4.11.1 does not make the allow_ptr_leaks value available for restricting the output of the print_bpf_insn function, which allows local users to obtain sensitive address information via crafted bpf system calls.
CVE-2017-9208	libqpdf.a in QPDF 6.0.0 allows remote attackers to cause a denial of service (infinite recursion and stack consumption) via a crafted PDF document, related to releaseResolved functions, aka qpdf-infiniteloop1.
CVE-2017-9209	libqpdf.a in QPDF 6.0.0 allows remote attackers to cause a denial of service (infinite recursion and stack consumption) via a crafted PDF document, related to QPDFObjectHandle::parseInternal, aka qpdf-infiniteloop2.
CVE-2017-9210	libqpdf.a in QPDF 6.0.0 allows remote attackers to cause a denial of service (infinite recursion and stack consumption) via a crafted PDF document, related to unparse functions, aka qpdf-infiniteloop3.
CVE-2017-9214	In Open vSwitch (OvS) 2.7.0, while parsing an OFPT_QUEUE_GET_CONFIG_REPLY type OFP 1.0 message, there is a buffer over-read that is caused by an unsigned integer underflow in the function `ofputil_pull_queue_get_config_reply10` in `lib/ofp-util.c`.
CVE-2017-9224	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds read occurs in match_at() during regular expression searching. A logical error involving order of validation and access in match_at() could result in an out-of-bounds read from a stack buffer.
CVE-2017-9226	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A heap out-of-bounds write or read occurs in next_state_val() during regular expression compilation. Octal numbers larger than

	0xff are not handled correctly in fetch_token() and fetch_token_in_cc(). A malformed regular expression containing an octal number in the form of '\700' would produce an invalid code point value larger than 0xff in next_state_val(), resulting in an out-of-bounds write memory corruption.
CVE-2017-9227	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A stack out-of-bounds read occurs in mbc_enc_len() during regular expression searching. Invalid handling of reg->dmin in forward_search_range() could result in an invalid pointer dereference, as an out-of-bounds read from a stack buffer.
CVE-2017-9228	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A heap out-of-bounds write occurs in bitset_set_range() during regular expression compilation due to an uninitialized variable from an incorrect state transition. An incorrect state transition in parse_char_class() could create an execution path that leaves a critical local variable uninitialized until it's used as an index, resulting in an out-of-bounds write memory corruption.
CVE-2017-9229	An issue was discovered in Oniguruma 6.2.0, as used in Oniguruma-mod in Ruby through 2.4.1 and mbstring in PHP through 7.1.5. A SIGSEGV occurs in left_adjust_char_head() during regular expression compilation. Invalid handling of reg->dmax in forward_search_range() could result in an invalid pointer dereference, normally as an immediate denial-of-service condition.
CVE-2017-9232	Juju before 1.25.12, 2.0.x before 2.0.4, and 2.1.x before 2.1.3 uses a UNIX domain socket without setting appropriate permissions, allowing privilege escalation by users on the system to root.
CVE-2017-9233	XML External Entity vulnerability in libexpat 2.2.0 and earlier (Expat XML Parser Library) allows attackers to put the parser in an infinite loop using a malformed external entity definition from an external DTD.
CVE-2017-9239	An issue was discovered in Exiv2 0.26. When the data structure of the structure ifd is incorrect, the program assigns pValue_ to 0x0, and the value of pValue() is 0x0. TiffImageEntry::doWriteImage will use the value of pValue() to cause a segmentation fault. To exploit this vulnerability, someone must open a crafted tiff file.
CVE-2017-9242	The __ip6_append_data function in net/ipv6/ip6_output.c in the Linux kernel through 4.11.3 is too late in checking whether an overwrite of an skb data structure may occur, which allows local users to cause

	a denial of service (system crash) via crafted system calls.
CVE-2017-9261	In ImageMagick 7.0.5-6 Q16, the ReadMNGImage function in coders/png.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-9262	In ImageMagick 7.0.5-6 Q16, the ReadJNGImage function in coders/png.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-9263	In Open vSwitch (OvS) 2.7.0, while parsing an OpenFlow role status message, there is a call to the abort() function for undefined role status reasons in the function `ofp_print_role_status_message` in `lib/ofp-print.c` that may be leveraged toward a remote DoS attack by a malicious switch.
CVE-2017-9264	In lib/conntrack.c in the firewall implementation in Open vSwitch (OvS) 2.6.1, there is a buffer over-read while parsing malformed TCP, UDP, and IPv6 packets in the functions `extract_l3_ipv6`, `extract_l4_tcp`, and `extract_l4_udp` that can be triggered remotely.
CVE-2017-9265	In Open vSwitch (OvS) v2.7.0, there is a buffer over-read while parsing the group mod OpenFlow message sent from the controller in `lib/ofp-util.c` in the function `ofputil_pull_ofp15_group_mod`.
CVE-2017-9287	servers/slapd/back-mdb/search.c in OpenLDAP through 2.4.44 is prone to a double free vulnerability. A user with access to search the directory can crash slapd by issuing a search including the Paged Results control with a page size of 0.
CVE-2017-9310	QEMU (aka Quick Emulator), when built with the e1000e NIC emulation support, allows local guest OS privileged users to cause a denial of service (infinite loop) via vectors related to setting the initial receive / transmit descriptor head (TDH/RDH) outside the allocated descriptor buffer.
CVE-2017-9330	QEMU (aka Quick Emulator) before 2.9.0, when built with the USB OHCI Emulation support, allows local guest OS users to cause a denial of service (infinite loop) by leveraging an incorrect return value, a different vulnerability than CVE-2017-6505.
CVE-2017-9373	Memory leak in QEMU (aka Quick Emulator), when built with IDE AHCI Emulation support, allows local guest OS privileged users to cause a denial of service (memory consumption) by repeatedly hot-unplugging the AHCI device.
CVE-2017-9374	Memory leak in QEMU (aka Quick Emulator), when built with USB EHCI Emulation support, allows local guest OS privileged users to cause a denial of service (memory consumption) by repeatedly hot-unplugging the device.

CVE-2017-9375	QEMU (aka Quick Emulator), when built with USB xHCI controller emulator support, allows local guest OS privileged users to cause a denial of service (infinite recursive call) via vectors involving control transfer descriptors sequencing.
CVE-2017-9403	In LibTIFF 4.0.7, a memory leak vulnerability was found in the function TIFFReadDirEntryLong8Array in tif_dirread.c, which allows attackers to cause a denial of service via a crafted file.
CVE-2017-9404	In LibTIFF 4.0.7, a memory leak vulnerability was found in the function OJPEGReadHeaderInfoSecTablesQTable in tif_ojpeg.c, which allows attackers to cause a denial of service via a crafted file.
CVE-2017-9405	In ImageMagick 7.0.5-5, the ReadICONImage function in icon.c:452 allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-9406	In Poppler 0.54.0, a memory leak vulnerability was found in the function gmalloc in gmem.cc, which allows attackers to cause a denial of service via a crafted file.
CVE-2017-9407	In ImageMagick 7.0.5-5, the ReadPALMImage function in palm.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-9408	In Poppler 0.54.0, a memory leak vulnerability was found in the function Object::initArray in Object.cc, which allows attackers to cause a denial of service via a crafted file.
CVE-2017-9409	In ImageMagick 7.0.5-5, the ReadMPCImage function in mpc.c allows attackers to cause a denial of service (memory leak) via a crafted file.
CVE-2017-9433	Document Liberation Project libmwaw before 2017-04-08 has an out-of-bounds write caused by a heap-based buffer overflow related to the MsWrd1Parser::readFootnoteCorrespondance function in lib/MsWrd1Parser.cxx.
CVE-2017-9439	In ImageMagick 7.0.5-5, a memory leak was found in the function ReadPDBImage in coders/pdb.c, which allows attackers to cause a denial of service via a crafted file.
CVE-2017-9440	In ImageMagick 7.0.5-5, a memory leak was found in the function ReadPSDChannel in coders/psd.c, which allows attackers to cause a denial of service via a crafted file.
CVE-2017-9461	smbd in Samba before 4.4.10 and 4.5.x before 4.5.6 has a denial of service vulnerability (fd_open_atomic infinite loop with high CPU usage and memory consumption) due to wrongly handling dangling symlinks.

CVE-2017-9468	In Irssi before 1.0.3, when receiving a DCC message without source nick/host, it attempts to dereference a NULL pointer. Thus, remote IRC servers can cause a crash.
CVE-2017-9469	In Irssi before 1.0.3, when receiving certain incorrectly quoted DCC files, it tries to find the terminating quote one byte before the allocated memory. Thus, remote attackers might be able to cause a crash.
CVE-2017-9501	In ImageMagick 7.0.5-7 Q16, an assertion failure was found in the function LockSemaphoreInfo, which allows attackers to cause a denial of service via a crafted file.
CVE-2017-9503	QEMU (aka Quick Emulator), when built with MegaRAID SAS 8708EM2 Host Bus Adapter emulation support, allows local guest OS privileged users to cause a denial of service (NULL pointer dereference and QEMU process crash) via vectors involving megasas command processing.
CVE-2017-9524	The qemu-nbd server in QEMU (aka Quick Emulator), when built with the Network Block Device (NBD) Server support, allows remote attackers to cause a denial of service (segmentation fault and server crash) by leveraging failure to ensure that all initialization occurs before talking to a client in the nbd_negotiate function.
CVE-2017-9526	In Libgcrypt before 1.7.7, an attacker who learns the EdDSA session key (from side-channel observation during the signing process) can easily recover the long-term secret key. 1.7.7 makes a cipher/ecc-eddsa.c change to store this session key in secure memory, to ensure that constant-time point operations are used in the MPI library.
CVE-2017-9605	The vmw_gb_surface_define_ioctl function (accessible via DRM_IOCTL_VMW_GB_SURFACE_CREATE) in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.11.4 defines a backup_handle variable but does not give it an initial value. If one attempts to create a GB surface, with a previously allocated DMA buffer to be used as a backup buffer, the backup_handle variable does not get written to and is then later returned to user space, allowing local users to obtain sensitive information from uninitialized kernel memory via a crafted ioctl call.
CVE-2017-9611	The Ins_MIRP function in base/ttinterp.c in Artifex Ghostscript GhostXPS 9.21 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.
CVE-2017-9612	The Ins_IP function in base/ttinterp.c in Artifex Ghostscript GhostXPS 9.21 allows remote attackers to cause a denial of service (use-after-free and application

	crash) or possibly have unspecified other impact via a crafted document.
CVE-2017-9726	The Ins_MDRP function in base/ttinterp.c in Artifex Ghostscript GhostXPS 9.21 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.
CVE-2017-9727	The gx_ttfReader__Read function in base/gxttfb.c in Artifex Ghostscript GhostXPS 9.21 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.
CVE-2017-9739	The Ins_JMPR function in base/ttinterp.c in Artifex Ghostscript GhostXPS 9.21 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact via a crafted document.
CVE-2017-9775	Stack buffer overflow in GfxState.cc in pdftocairo in Poppler before 0.56 allows remote attackers to cause a denial of service (application crash) via a crafted PDF document.
CVE-2017-9776	Integer overflow leading to Heap buffer overflow in JBIG2Stream.cc in pdftocairo in Poppler before 0.56 allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PDF document.
CVE-2017-9788	In Apache httpd before 2.2.34 and 2.4.x before 2.4.27, the value placeholder in [Proxy-]Authorization headers of type 'Digest' was not initialized or reset before or between successive key=value assignments by mod_auth_digest. Providing an initial key with no '=' assignment could reflect the stale value of uninitialized pool memory used by the prior request, leading to leakage of potentially confidential information, and a segfault in other cases resulting in denial of service.
CVE-2017-9798	Apache httpd allows remote attackers to read secret data from process memory if the Limit directive can be set in a user's .htaccess file, or if httpd.conf has certain misconfigurations, aka Optionsbleed. This affects the Apache HTTP Server through 2.2.34 and 2.4.x through 2.4.27. The attacker sends an unauthenticated OPTIONS HTTP request when attempting to read secret data. This is a use-after-free issue and thus secret data is not always sent, and the specific data depends on many factors including configuration. Exploitation with .htaccess can be blocked with a patch to the ap_limit_section function in server/core.c.
CVE-2017-9800	A maliciously constructed svn+ssh:// URL would cause Subversion clients before 1.8.19, 1.9.x before 1.9.7, and 1.10.0.x through 1.10.0-alpha3 to run an arbitrary

	shell command. Such a URL could be generated by a malicious server, by a malicious user committing to a honest server (to attack another user of that server's repositories), or by a proxy server. The vulnerability affects all clients, including those that use file://, http://, and plain (untunneled) svn://.
CVE-2017-9815	In LibTIFF 4.0.7, the TIFFReadDirEntryLong8Array function in libtiff/tif_dirread.c mishandles a malloc operation, which allows attackers to cause a denial of service (memory leak within the function _TIFFmalloc in tif_unix.c) via a crafted file.
CVE-2017-9835	The gs_alloc_ref_array function in psi/ialloc.c in Artifex Ghostscript 9.21 allows remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted PostScript document. This is related to a lack of an integer overflow check in base/gsalloc.c.
CVE-2017-9935	In LibTIFF 4.0.8, there is a heap-based buffer overflow in the t2p_write_pdf function in tools/tiff2pdf.c. This heap overflow could lead to different damages. For example, a crafted TIFF document can lead to an out-of-bounds read in TIFFCleanup, an invalid free in TIFFClose or t2p_free, memory corruption in t2p_readwrite_pdf_image, or a double free in t2p_free. Given these possibilities, it probably could cause arbitrary code execution.
CVE-2017-9936	In LibTIFF 4.0.8, there is a memory leak in tif_jbig.c. A crafted TIFF document can lead to a memory leak resulting in a remote denial of service attack.
CVE-2017-9951	The try_read_command function in memcached.c in memcached before 1.4.39 allows remote attackers to cause a denial of service (segmentation fault) via a request to add/set a key, which makes a comparison between signed and unsigned int and triggers a heap-based buffer over-read. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-8705.
CVE-2017-9984	The snd_msnd_interrupt function in sound/isa/msnd/msnd_pinnacle.c in the Linux kernel through 4.11.7 allows local users to cause a denial of service (over-boundary access) or possibly have unspecified other impact by changing the value of a message queue head pointer between two kernel reads of that value, aka a "double fetch" vulnerability.
CVE-2017-9985	The snd_msndmidi_input_read function in sound/isa/msnd/msnd_midi.c in the Linux kernel through 4.11.7 allows local users to cause a denial of service (over-boundary access) or possibly have unspecified other impact by changing the value of a message queue head

	pointer between two kernel reads of that value, aka a "double fetch" vulnerability.
CVE-2018-0202	clamscan in ClamAV before 0.99.4 contains a vulnerability that could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper input validation checking mechanisms when handling Portable Document Format (.pdf) files sent to an affected device. An unauthenticated, remote attacker could exploit this vulnerability by sending a crafted .pdf file to an affected device. This action could cause an out-of-bounds read when ClamAV scans the malicious file, allowing the attacker to cause a DoS condition. This concerns pdf_parse_array and pdf_parse_string in libclamav/pdfng.c. Cisco Bug IDs: CSCvh91380, CSCvh91400.
CVE-2018-0360	ClamAV before 0.100.1 has an HWP integer overflow with a resultant infinite loop via a crafted Hangul Word Processor file. This is in parsehwp3_paragraph() in libclamav/hwp.c.
CVE-2018-0361	ClamAV before 0.100.1 lacks a PDF object length check, resulting in an unreasonably long time to parse a relatively small file.
CVE-2018-0494	GNU Wget before 1.19.5 is prone to a cookie injection vulnerability in the resp_new function in http.c via a \r\n sequence in a continuation line.
CVE-2018-0495	Libgcrypt before 1.7.10 and 1.8.x before 1.8.3 allows a memory-cache side-channel attack on ECDSA signatures that can be mitigated through the use of blinding during the signing process in the _gcry_ecc_ecdsa_sign function in cipher/ecc-ecdsa.c, aka the Return Of the Hidden Number Problem or ROHNP. To discover an ECDSA key, the attacker needs access to either the local machine or a different virtual machine on the same physical host.
CVE-2018-0502	An issue was discovered in zsh before 5.6. The beginning of a #! script file was mishandled, potentially leading to an execve call to a program named on the second line.
CVE-2018-0732	During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).
CVE-2018-0734	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-2018-0735	The OpenSSL ECDSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.1.1a (Affected 1.1.1).
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-2018-1000001	In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the destination buffer leading to a buffer underflow and potential code execution.
CVE-2018-1000004	In the Linux kernel 4.12, 3.10, 2.6 and possibly earlier versions a race condition vulnerability exists in the sound system, this can lead to a deadlock and denial of service condition.
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 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.

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-2018-1000021	GIT version 2.15.1 and earlier contains a Input Validation Error vulnerability in Client that can result in problems including messing up terminal configuration to RCE. This attack appear to be exploitable via The user must interact with a malicious git server, (or have their traffic modified in a MITM attack).
CVE-2018-1000024	The Squid Software Foundation Squid HTTP Caching Proxy version 3.0 to 3.5.27, 4.0 to 4.0.22 contains a Incorrect Pointer Handling vulnerability in ESI Response Processing that can result in Denial of Service for all clients using the proxy.. This attack appear to be exploitable via Remote server delivers an HTTP response payload containing valid but unusual ESI syntax.. This vulnerability appears to have been fixed in 4.0.23 and later.
CVE-2018-1000026	Linux Linux kernel version at least v4.8 onwards, probably well before contains a Insufficient input validation vulnerability in bnx2x network card driver that can result in DoS: Network card firmware assertion takes card off-line. This attack appear to be exploitable via An attacker on a must pass a very large, specially crafted packet to the bnx2x card. This can be done from an untrusted guest VM..
CVE-2018-1000027	The Squid Software Foundation Squid HTTP Caching Proxy version prior to version 4.0.23 contains a NULL Pointer Dereference vulnerability in HTTP Response X-Forwarded-For header processing that can result in Denial of Service to all clients of the proxy. This attack appear to be exploitable via Remote HTTP server responding with an X-Forwarded-For header to certain types of HTTP request. This vulnerability appears to have been fixed in 4.0.23 and later.
CVE-2018-1000030	Python 2.7.14 is vulnerable to a Heap-Buffer-Overflow as well as a Heap-Use-After-Free. Python versions prior to 2.7.14 may also be vulnerable and it appears that Python 2.7.17 and prior may also be vulnerable however this has not been confirmed. The vulnerability lies when multiply threads are handling large amounts

	of data. In both cases there is essentially a race condition that occurs. For the Heap-Buffer-Overflow, Thread 2 is creating the size for a buffer, but Thread1 is already writing to the buffer without knowing how much to write. So when a large amount of data is being processed, it is very easy to cause memory corruption using a Heap-Buffer-Overflow. As for the Use-After-Free, Thread3->Malloc->Thread1->Free's->Thread2-Re-uses-Free'd Memory. The PSRT has stated that this is not a security vulnerability due to the fact that the attacker must be able to run code, however in some situations, such as function as a service, this vulnerability can potentially be used by an attacker to violate a trust boundary, as such the DWF feels this issue deserves a CVE.
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-2018-1000085	ClamAV version version 0.99.3 contains a Out of bounds heap memory read vulnerability in XAR parser, function xar_hash_check() that can result in Leaking of memory, may help in developing exploit chains.. This attack appear to be exploitable via The victim must scan a crafted XAR file. This vulnerability appears to have been fixed in after commit d96a6b8bcc7439fa7e3876207aa0a8e79c8451b6.
CVE-2018-1000097	Sharutils sharutils (unshar command) version 4.15.2 contains a Buffer Overflow vulnerability in Affected component on the file unshar.c at line 75, function looks_like_c_code. Failure to perform checking of the buffer containing input line. that can result in Could lead to code execution. This attack appear to be exploitable via Victim have to run unshar command on a specially crafted file..
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-2018-1000120	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-2018-1000127	memcached version prior to 1.4.37 contains an Integer Overflow vulnerability in items.c:item_free() that can result in data corruption and deadlocks due to items existing in hash table being reused from free list. This attack appear to be exploitable via network connectivity to the memcached service. This vulnerability appears to have been fixed in 1.4.37 and later.
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-2018-1000199	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-2018-1000200	The Linux Kernel versions 4.14, 4.15, and 4.16 has a null pointer dereference which can result in an out of memory (OOM) killing of large mlocked processes. The issue arises from an oom killed process's final thread calling exit_mmap(), which calls munlock_vma_pages_all() for mlocked vmas.This can happen synchronously with the oom reaper's unmap_page_range() since the vma's VM_LOCKED bit is cleared before munlocking (to determine if any other vmas share the memory and are mlocked).
CVE-2018-1000204	** DISPUTED ** Linux Kernel version 3.18 to 4.16 incorrectly handles an SG_IO ioctl on /dev/sg0 with dxfer_direction=SG_DXFER_FROM_DEV and an empty 6-byte cmdp. This may lead to copying up to 1000 kernel heap pages to the userspace. This has been fixed upstream in https://github.com/torvalds/linux/commit/a45b599ad808c3c982fdcdc12b0b8611c2f92824

	already. The problem has limited scope, as users don't usually have permissions to access SCSI devices. On the other hand, e.g. the Nero user manual suggests doing `chmod o+r+w /dev/sg*` to make the devices accessible. NOTE: third parties dispute the relevance of this report, noting that the requirement for an attacker to have both the CAP_SYS_ADMIN and CAP_SYS_RAWIO capabilities makes it "virtually impossible to exploit."
CVE-2018-1000222	Libgd version 2.2.5 contains a Double Free Vulnerability vulnerability in gdImageBmpPtr Function that can result in Remote Code Execution . This attack appear to be exploitable via Specially Crafted Jpeg Image can trigger double free. This vulnerability appears to have been fixed in after commit ac16bdf2d41724b5a65255d4c28fb0ec46bc42f5.
CVE-2018-1000300	curl version curl 7.54.1 to and including curl 7.59.0 contains a CWE-122: Heap-based Buffer Overflow vulnerability in denial of service and more that can result in curl might overflow a heap based memory buffer when closing down an FTP connection with very long server command replies.. This vulnerability appears to have been fixed in curl < 7.54.1 and curl >= 7.60.0.
CVE-2018-1000301	curl version curl 7.20.0 to and including curl 7.59.0 contains a CWE-126: Buffer Over-read vulnerability in denial of service that can result in curl can be tricked into reading data beyond the end of a heap based buffer used to store downloaded RTSP content.. This vulnerability appears to have been fixed in curl < 7.20.0 and curl >= 7.60.0.
CVE-2018-1000802	Python Software Foundation Python (CPython) version 2.7 contains a CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in shutil module (make_archive function) that can result in Denial of service, Information gain via injection of arbitrary files on the system or entire drive. This attack appear to be exploitable via Passage of unfiltered user input to the function. This vulnerability appears to have been fixed in after commit add531a1e55b0a739b0f42582f1c9747e5649ace.
CVE-2018-1000805	Paramiko version 2.4.1, 2.3.2, 2.2.3, 2.1.5, 2.0.8, 1.18.5, 1.17.6 contains a Incorrect Access Control vulnerability in SSH server that can result in RCE. This attack appear to be exploitable via network connectivity.
CVE-2018-1000807	Python Cryptographic Authority pyopenssl version prior to version 17.5.0 contains a CWE-416: Use After Free vulnerability in X509 object handling that can result in Use after free can lead to possible denial of service or remote code execution.. This attack appear to be exploitable via Depends on the calling application and if

	it retains a reference to the memory.. This vulnerability appears to have been fixed in 17.5.0.
CVE-2018-1000808	Python Cryptographic Authority pyopenssl version Before 17.5.0 contains a CWE - 401 : Failure to Release Memory Before Removing Last Reference vulnerability in PKCS #12 Store that can result in Denial of service if memory runs low or is exhausted. This attack appear to be exploitable via Depends upon calling application, however it could be as simple as initiating a TLS connection. Anything that would cause the calling application to reload certificates from a PKCS #12 store.. This vulnerability appears to have been fixed in 17.5.0.
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-2018-1000880	libarchive version commit 9693801580c0cf7c70e862d305270a16b52826a7 onwards (release v3.2.0 onwards) contains a CWE-20: Improper Input Validation vulnerability in WARC parser - libarchive/archive_read_support_format_warc.c, _warc_read() that can result in DoS - quasi-infinite run time and disk usage from tiny file. This attack appear to be exploitable via the victim must open a specially crafted WARC file.
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-2018-10021	** DISPUTED ** drivers/scsi/libsas/sas_scsi_host.c in the Linux kernel before 4.16 allows local users to cause a denial of service (ata qc leak) by triggering certain failure conditions. NOTE: a third party disputes the relevance of this report because the failure can only occur for physically proximate attackers who unplug SAS Host Bus Adapter cables.
CVE-2018-1002105	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-2018-10087	The kernel_wait4 function in kernel/exit.c in the Linux kernel before 4.13, when an unspecified architecture and compiler is used, might allow local users to cause a denial of service by triggering an attempted use of the -INT_MIN value.
CVE-2018-10119	sot/source/sdstor/stgstrms.cxx in LibreOffice before 5.4.5.1 and 6.x before 6.0.1.1 uses an incorrect integer data type in the StgSmallStrm class, which allows remote attackers to cause a denial of service (use-after-free with write access) or possibly have unspecified other impact via a crafted document that uses the structured storage ole2 wrapper file format.
CVE-2018-10120	The SwCTBWrapper::Read function in sw/source/filter/ww8/ww8toolbar.cxx in LibreOffice before 5.4.6.1 and 6.x before 6.0.2.1 does not validate a customizations index, which allows remote attackers to cause a denial of service (heap-based buffer overflow with write access) or possibly have unspecified other impact via a crafted document that contains a certain Microsoft Word record.
CVE-2018-10124	The kill_something_info function in kernel/signal.c in the Linux kernel before 4.13, when an unspecified architecture and compiler is used, might allow local users to cause a denial of service via an INT_MIN argument.
CVE-2018-10177	In ImageMagick 7.0.7-28, there is an infinite loop in the ReadOneMNGImage function of the coders/png.c file. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted mng file.

CVE-2018-10194	The set_text_distance function in devices/vector/gdevpdts.c in the pdfwrite component in Artifex Ghostscript through 9.22 does not prevent overflows in text-positioning calculation, which allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a crafted PDF document.
CVE-2018-10196	NULL pointer dereference vulnerability in the rebuild_vlists function in lib/dotgen/conc.c in the dotgen library in Graphviz 2.40.1 allows remote attackers to cause a denial of service (application crash) via a crafted file.
CVE-2018-10323	The xfs_bmap_extents_to_btree function in fs/xfs/libxfs/xfs_bmap.c in the Linux kernel through 4.16.3 allows local users to cause a denial of service (xfs_bmapi_write NULL pointer dereference) via a crafted xfs image.
CVE-2018-10360	The do_core_note function in readelf.c in libmagic.a in file 5.33 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted ELF file.
CVE-2018-1049	In systemd prior to 234 a race condition exists between .mount and .automount 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-2018-10528	An issue was discovered in LibRaw 0.18.9. There is a stack-based buffer overflow in the utf2char function in libraw_cxx.cpp.
CVE-2018-10529	An issue was discovered in LibRaw 0.18.9. There is an out-of-bounds read affecting the X3F property table list implementation in libraw_x3f.cpp and libraw_cxx.cpp.
CVE-2018-1053	In postgresql 9.3.x before 9.3.21, 9.4.x before 9.4.16, 9.5.x before 9.5.11, 9.6.x before 9.6.7 and 10.x before 10.2, pg_upgrade creates file in current working directory containing the output of `pg_dumpall -g` under umask which was in effect when the user invoked pg_upgrade, and not under 0077 which is normally used for other temporary files. This can allow an authenticated attacker to read or modify the one file, which may contain encrypted or unencrypted database passwords. The attack is infeasible if a directory mode

	blocks the attacker searching the current working directory or if the prevailing umask blocks the attacker opening the file.
CVE-2018-10545	An issue was discovered in PHP before 5.6.35, 7.0.x before 7.0.29, 7.1.x before 7.1.16, and 7.2.x before 7.2.4. Dumpable FPM child processes allow bypassing opcache access controls because fpm_unix.c makes a PR_SET_DUMPABLE prctl call, allowing one user (in a multiuser environment) to obtain sensitive information from the process memory of a second user's PHP applications by running gcore on the PID of the PHP-FPM worker process.
CVE-2018-10546	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. An infinite loop exists in ext/iconv/iconv.c because the iconv stream filter does not reject invalid multibyte sequences.
CVE-2018-10547	An issue was discovered in ext/phar/phar_object.c in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. There is Reflected XSS on the PHAR 403 and 404 error pages via request data of a request for a .phar file. NOTE: this vulnerability exists because of an incomplete fix for CVE-2018-5712.
CVE-2018-10548	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. ext/ldap/ldap.c allows remote LDAP servers to cause a denial of service (NULL pointer dereference and application crash) because of mishandling of the ldap_get_dn return value.
CVE-2018-10549	An issue was discovered in PHP before 5.6.36, 7.0.x before 7.0.30, 7.1.x before 7.1.17, and 7.2.x before 7.2.5. exif_read_data in ext/exif/exif.c has an out-of-bounds read for crafted JPEG data because exif_iif_add_value mishandles the case of a MakerNote that lacks a final '\0' character.
CVE-2018-1056	An out-of-bounds heap buffer read flaw was found in the way advancecomp before 2.1-2018/02 handled processing of ZIP files. An attacker could potentially use this flaw to crash the advzip utility by tricking it into processing crafted ZIP files.
CVE-2018-1057	On a Samba 4 AD DC the LDAP server in all versions of Samba from 4.0.0 onwards incorrectly validates permissions to modify passwords over LDAP allowing authenticated users to change any other users' passwords, including administrative users and privileged service accounts (eg Domain Controllers).
CVE-2018-1058	A flaw was found in the way Postgresql allowed a user to modify the behavior of a query for other users. An attacker with a user account could use this flaw to

	execute code with the permissions of superuser in the database. Versions 9.3 through 10 are affected.
CVE-2018-10583	An information disclosure vulnerability occurs when LibreOffice 6.0.3 and Apache OpenOffice Writer 4.1.5 automatically process and initiate an SMB connection embedded in a malicious file, as demonstrated by xlink:href=file://192.168.0.2/test.jpg within an office:document-content element in a .odt XML document.
CVE-2018-1060	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 pop3lib's apop() 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-2018-1064	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-2018-1065	The netfilter subsystem in the Linux kernel through 4.15.7 mishandles the case of a rule blob that contains a jump but lacks a user-defined chain, which allows local users to cause a denial of service (NULL pointer dereference) by leveraging the CAP_NET_RAW or CAP_NET_ADMIN capability, related to arpt_do_table in net/ipv4/netfilter/arp_tables.c, ipt_do_table in net/ipv4/netfilter/ip_tables.c, and ip6t_do_table in net/ipv6/netfilter/ip6_tables.c.
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-2018-1071	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-2018-10768	There is a NULL pointer dereference in the AnnotPath::getCoordsLength function in Annot.h in an Ubuntu package for Poppler 0.24.5. A crafted input will lead to a remote denial of service attack. Later Ubuntu packages such as for Poppler 0.41.0 are not affected.
CVE-2018-10804	ImageMagick version 7.0.7-28 contains a memory leak in WriteTIFFImage in coders/tiff.c.
CVE-2018-10805	ImageMagick version 7.0.7-28 contains a memory leak in ReadYCBCRImage in coders/ycbcr.c.
CVE-2018-10811	strongSwan 5.6.0 and older allows Remote Denial of Service because of Missing Initialization of a Variable.

CVE-2018-1083	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-2018-10839	Qemu emulator <= 3.0.0 built with the NE2000 NIC emulation support is vulnerable to an integer overflow, which could lead to buffer overflow issue. It could occur when receiving packets over the network. A user inside guest could use this flaw to crash the Qemu process resulting in DoS.
CVE-2018-10840	Linux kernel is vulnerable to a heap-based buffer overflow in the fs/ext4/xattr.c:ext4_xattr_set_entry() function. An attacker could exploit this by operating on a mounted crafted ext4 image.
CVE-2018-10853	A flaw was found in the way Linux kernel KVM hypervisor before 4.18 emulated instructions such as sgdt/sidt/fxsave/fxrstor. It did not check current privilege(CPL) level while emulating unprivileged instructions. An unprivileged guest user/process could use this flaw to potentially escalate privileges inside guest.
CVE-2018-10858	A heap-buffer overflow was found in the way samba clients processed extra long filename in a directory listing. A malicious samba server could use this flaw to cause arbitrary code execution on a samba client. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.
CVE-2018-10860	perl-archive-zip is vulnerable to a directory traversal in Archive::Zip. It was found that the Archive::Zip module did not properly sanitize paths while extracting zip files. An attacker able to provide a specially crafted archive for processing could use this flaw to write or overwrite arbitrary files in the context of the perl interpreter.
CVE-2018-1087	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-2018-10876	A flaw was found in Linux kernel in the ext4 filesystem code. A use-after-free is possible in

	ext4_ext_remove_space() function when mounting and operating a crafted ext4 image.
CVE-2018-10877	Linux kernel ext4 filesystem is vulnerable to an out-of-bound access in the ext4_ext_drop_refs() function when operating on a crafted ext4 filesystem image.
CVE-2018-10878	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bounds write and a denial of service or unspecified other impact is possible by mounting and operating a crafted ext4 filesystem image.
CVE-2018-10879	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause a use-after-free in ext4_xattr_set_entry function and a denial of service or unspecified other impact may occur by renaming a file in a crafted ext4 filesystem image.
CVE-2018-10881	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bound access in ext4_get_group_info function, a denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.
CVE-2018-10882	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bound write in in fs/jbd2/transaction.c code, a denial of service, and a system crash by unmounting a crafted ext4 filesystem image.
CVE-2018-10902	It was found that the raw midi kernel driver does not protect against concurrent access which leads to a double realloc (double free) in snd_rawmidi_input_params() and snd_rawmidi_output_status() which are part of snd_rawmidi_ioctl() handler in rawmidi.c file. A malicious local attacker could possibly use this for privilege escalation.
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-2018-10919	The Samba Active Directory LDAP server was vulnerable to an information disclosure flaw because of missing access control checks. An authenticated attacker could use this flaw to extract confidential attribute values using LDAP search expressions. Samba versions before 4.6.16, 4.7.9 and 4.8.4 are vulnerable.

CVE-2018-1092	The ext4_iget function in fs/ext4/inode.c in the Linux kernel through 4.15.15 mishandles the case of a root directory with a zero i_links_count, which allows attackers to cause a denial of service (ext4_process_freed_data NULL pointer dereference and OOPS) via a crafted ext4 image.
CVE-2018-10925	It was discovered that PostgreSQL versions before 10.5, 9.6.10, 9.5.14, 9.4.19, and 9.3.24 failed to properly check authorization on certain statements involved with "INSERT ... ON CONFLICT DO UPDATE". An attacker with "CREATE TABLE" privileges could exploit this to read arbitrary bytes server memory. If the attacker also had certain "INSERT" and limited "UPDATE" privileges to a particular table, they could exploit this to update other columns in the same table.
CVE-2018-1093	The ext4_valid_block_bitmap function in fs/ext4/balloc.c in the Linux kernel through 4.15.15 allows attackers to cause a denial of service (out-of-bounds read and system crash) via a crafted ext4 image because balloc.c and ialloc.c do not validate bitmap block numbers.
CVE-2018-10933	A vulnerability was found in libssh's server-side state machine before versions 0.7.6 and 0.8.4. A malicious client could create channels without first performing authentication, resulting in unauthorized access.
CVE-2018-10938	A flaw was found in the Linux kernel present since v4.0-rc1 and through v4.13-rc4. A crafted network packet sent remotely by an attacker may force the kernel to enter an infinite loop in the cipso_v4_optptr() function in net/ipv4/cipso_ipv4.c leading to a denial-of-service. A certain non-default configuration of LSM (Linux Security Module) and NetLabel should be set up on a system before an attacker could leverage this flaw.
CVE-2018-1094	The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.15.15 does not always initialize the crc32c checksum driver, which allows attackers to cause a denial of service (ext4_xattr_inode_hash NULL pointer dereference and system crash) via a crafted ext4 image.
CVE-2018-10940	The cdrom_ioctl_media_changed function in drivers/cdrom/cdrom.c in the Linux kernel before 4.16.6 allows local attackers to use a incorrect bounds check in the CDROM driver CDROM_MEDIA_CHANGED ioctl to read out kernel memory.
CVE-2018-1095	The ext4_xattr_check_entries function in fs/ext4/xattr.c in the Linux kernel through 4.15.15 does not properly validate xattr sizes, which causes misinterpretation of a size as an error code, and consequently allows attackers to cause a denial of service (get_acl NULL

	pointer dereference and system crash) via a crafted ext4 image.
CVE-2018-10958	In types.cpp in Exiv2 0.26, a large size value may lead to a SIGABRT during an attempt at memory allocation for an Exiv2::Internal::PngChunk::zlibUncompress call.
CVE-2018-10963	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-2018-10999	An issue was discovered in Exiv2 0.26. The Exiv2::Internal::PngChunk::parseTXTChunk function has a heap-based buffer over-read.
CVE-2018-1100	zsh through version 5.4.2 is vulnerable to a stack-based buffer overflow in the utils.c:checkmailpath function. A local attacker could exploit this to execute arbitrary code in the context of another user.
CVE-2018-1108	kernel drivers before version 4.17-rc1 are vulnerable to a weakness in the Linux kernel's implementation of random seed data. Programs, early in the boot sequence, could use the data allocated for the seed before it was sufficiently generated.
CVE-2018-1116	A flaw was found in polkit before version 0.116. The implementation of the polkit_backend_interactive_authority_check_authorization function in polkitd allows to test for authentication and trigger authentication of unrelated processes owned by other users. This may result in a local DoS and information disclosure.
CVE-2018-1118	Linux kernel vhost since version 4.8 does not properly initialize memory in messages passed between virtual guests and the host operating system in the vhost/vhost.c:vhost_new_msg() function. This can allow local privileged users to read some kernel memory contents when reading from the /dev/vhost-net device file.
CVE-2018-1120	A flaw was found affecting the Linux kernel before version 4.17. By mmap()ing a FUSE-backed file onto a process's memory containing command line arguments (or environment strings), an attacker can cause utilities from psutils or procps (such as ps, w) or any other program which makes a read() call to the /proc/<pid>/cmdline (or /proc/<pid>/environ) files to block indefinitely (denial of service) or for some controlled time (as a synchronization primitive for other attacks).

CVE-2018-11212	An issue was discovered in libjpeg 9a. The alloc_sarray function in jmemmgr.c allows remote attackers to cause a denial of service (divide-by-zero error) via a crafted file.
CVE-2018-11213	An issue was discovered in libjpeg 9a. The get_text_gray_row function in rdppm.c allows remote attackers to cause a denial of service (Segmentation fault) via a crafted file.
CVE-2018-11214	An issue was discovered in libjpeg 9a. The get_text_rgb_row function in rdppm.c allows remote attackers to cause a denial of service (Segmentation fault) via a crafted file.
CVE-2018-1122	procps-ng before version 3.3.15 is vulnerable to a local privilege escalation in top. If a user runs top with HOME unset in an attacker-controlled directory, the attacker could achieve privilege escalation by exploiting one of several vulnerabilities in the config_file() function.
CVE-2018-1123	procps-ng before version 3.3.15 is vulnerable to a denial of service in ps via mmap buffer overflow. Inbuilt protection in ps maps a guard page at the end of the overflowed buffer, ensuring that the impact of this flaw is limited to a crash (temporary denial of service).
CVE-2018-11233	In Git before 2.13.7, 2.14.x before 2.14.4, 2.15.x before 2.15.2, 2.16.x before 2.16.4, and 2.17.x before 2.17.1, code to sanity-check pathnames on NTFS can result in reading out-of-bounds memory.
CVE-2018-11235	In Git before 2.13.7, 2.14.x before 2.14.4, 2.15.x before 2.15.2, 2.16.x before 2.16.4, and 2.17.x before 2.17.1, remote code execution can occur. With a crafted .gitmodules file, a malicious project can execute an arbitrary script on a machine that runs "git clone --recurse-submodules" because submodule "names" are obtained from this file, and then appended to $GIT_DIR/modules, leading to directory traversal with "../" in a name. Finally, post-checkout hooks from a submodule are executed, bypassing the intended design in which hooks are not obtained from a remote server.
CVE-2018-1124	procps-ng before version 3.3.15 is vulnerable to multiple integer overflows leading to a heap corruption in file2strvec function. This allows a privilege escalation for a local attacker who can create entries in procfs by starting processes, which could result in crashes or arbitrary code execution in proc utilities run by other users.
CVE-2018-1125	procps-ng before version 3.3.15 is vulnerable to a stack buffer overflow in pgrep. This vulnerability is mitigated by FORTIFY, as it involves strncat() to a stack-allocated string. When pgrep is compiled with FORTIFY (as on

	Red Hat Enterprise Linux and Fedora), the impact is limited to a crash.
CVE-2018-11251	In ImageMagick 7.0.7-23 Q16 x86_64 2018-01-24, there is a heap-based buffer over-read in ReadSUNImage in coders/sun.c, which allows attackers to cause a denial of service (application crash in SetGrayscaleImage in MagickCore/quantize.c) via a crafted SUN image file.
CVE-2018-1126	procps-ng before version 3.3.15 is vulnerable to an incorrect integer size in proc/alloc.* leading to truncation/integer overflow issues. This flaw is related to CVE-2018-1124.
CVE-2018-1130	Linux kernel before version 4.16-rc7 is vulnerable to a null pointer dereference in dccp_write_xmit() function in net/dccp/output.c in that allows a local user to cause a denial of service by a number of certain crafted system calls.
CVE-2018-11410	An issue was discovered in Liblouis 3.5.0. A invalid free in the compileRule function in compileTranslationTable.c allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact.
CVE-2018-11412	In the Linux kernel 4.13 through 4.16.11, ext4_read_inline_data() in fs/ext4/inline.c performs a memcpy with an untrusted length value in certain circumstances involving a crafted filesystem that stores the system.data extended attribute value in a dedicated inode.
CVE-2018-11440	Liblouis 3.5.0 has a stack-based Buffer Overflow in the function parseChars in compileTranslationTable.c.
CVE-2018-11506	The sr_do_ioctl function in drivers/scsi/sr_ioctl.c in the Linux kernel through 4.16.12 allows local users to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact because sense buffers have different sizes at the CDROM layer and the SCSI layer, as demonstrated by a CDROMREADMODE2 ioctl call.
CVE-2018-11508	The compat_get_timex function in kernel/compat.c in the Linux kernel before 4.16.9 allows local users to obtain sensitive information from kernel memory via adjtimex.
CVE-2018-1152	libjpeg-turbo 1.5.90 is vulnerable to a denial of service vulnerability caused by a divide by zero when processing a crafted BMP image.
CVE-2018-11531	Exiv2 0.26 has a heap-based buffer overflow in getData in preview.cpp.
CVE-2018-11574	Improper input validation together with an integer overflow in the EAP-TLS protocol implementation in PPPD may cause a crash, information disclosure,

	or authentication bypass. This implementation is distributed as a patch for PPPD 0.91, and includes the affected eap.c and eap-tls.c files. Configurations that use the `refuse-app` option are unaffected.
CVE-2018-11577	Liblouis 3.5.0 has a Segmentation fault in lou_logPrint in logging.c.
CVE-2018-11625	In ImageMagick 7.0.7-37 Q16, SetGrayscaleImage in the quantize.c file allows attackers to cause a heap-based buffer over-read via a crafted file.
CVE-2018-11645	psi/zfile.c in Artifex Ghostscript before 9.21rc1 permits the status command even if -dSAFER is used, which might allow remote attackers to determine the existence and size of arbitrary files, a similar issue to CVE-2016-7977.
CVE-2018-11655	In ImageMagick 7.0.7-20 Q16 x86_64, a memory leak vulnerability was found in the function GetImagePixelCache in MagickCore/cache.c, which allows attackers to cause a denial of service via a crafted CALS image file.
CVE-2018-11656	In ImageMagick 7.0.7-20 Q16 x86_64, a memory leak vulnerability was found in the function ReadDCMImage in coders/dcm.c, which allows attackers to cause a denial of service via a crafted DCM image file.
CVE-2018-11683	Liblouis 3.5.0 has a stack-based Buffer Overflow in the function parseChars in compileTranslationTable.c, a different vulnerability than CVE-2018-11440.
CVE-2018-11684	Liblouis 3.5.0 has a stack-based Buffer Overflow in the function includeFile in compileTranslationTable.c.
CVE-2018-11685	Liblouis 3.5.0 has a stack-based Buffer Overflow in the function compileHyphenation in compileTranslationTable.c.
CVE-2018-11780	A potential Remote Code Execution bug exists with the PDFInfo plugin in Apache SpamAssassin before 3.4.2.
CVE-2018-11781	Apache SpamAssassin 3.4.2 fixes a local user code injection in the meta rule syntax.
CVE-2018-11784	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-2018-11790	When loading a document with Apache Open Office 4.1.5 and earlier with smaller end line termination than the operating system uses, the defect occurs. In this case OpenOffice runs into an Arithmetic Overflow at a string length calculation.
CVE-2018-11806	m_cat in slirp/mbuf.c in Qemu has a heap-based buffer overflow via incoming fragmented datagrams.

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

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

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

	arbitrary code. This vulnerability affects Firefox < 62, Firefox ESR < 60.2, and Thunderbird < 60.2.1.
CVE-2018-12377	A use-after-free vulnerability can occur when refresh driver timers are refreshed in some circumstances during shutdown when the timer is deleted while still in use. This results in a potentially exploitable crash. This vulnerability affects Firefox < 62, Firefox ESR < 60.2, and Thunderbird < 60.2.1.
CVE-2018-12378	A use-after-free vulnerability can occur when an IndexedDB index is deleted while still in use by JavaScript code that is providing payload values to be stored. This results in a potentially exploitable crash. This vulnerability affects Firefox < 62, Firefox ESR < 60.2, and Thunderbird < 60.2.1.
CVE-2018-12383	If a user saved passwords before Firefox 58 and then later set a master password, an unencrypted copy of these passwords is still accessible. This is because the older stored password file was not deleted when the data was copied to a new format starting in Firefox 58. The new master password is added only on the new file. This could allow the exposure of stored password data outside of user expectations. This vulnerability affects Firefox < 62, Firefox ESR < 60.2.1, and Thunderbird < 60.2.1.
CVE-2018-12384	A flaw was found in the way NSS responded to an SSLv2-compatible ClientHello with a ServerHello that had an all-zero random. A man-in-the-middle attacker could use this flaw in a passive replay attack.
CVE-2018-12385	A potentially exploitable crash in TransportSecurityInfo used for SSL can be triggered by data stored in the local cache in the user profile directory. This issue is only exploitable in combination with another vulnerability allowing an attacker to write data into the local cache or from locally installed malware. This issue also triggers a non-exploitable startup crash for users switching between the Nightly and Release versions of Firefox if the same profile is used. This vulnerability affects Thunderbird < 60.2.1, Firefox ESR < 60.2.1, and Firefox < 62.0.2.
CVE-2018-12386	A vulnerability in register allocation in JavaScript can lead to type confusion, allowing for an arbitrary read and write. This leads to remote code execution inside the sandboxed content process when triggered. This vulnerability affects Firefox ESR < 60.2.2 and Firefox < 62.0.3.
CVE-2018-12387	A vulnerability where the JavaScript JIT compiler inlines Array.prototype.push with multiple arguments that results in the stack pointer being off by 8 bytes after a bailout. This leaks a memory address to the calling function which can be used as part of an exploit inside

	the sandboxed content process. This vulnerability affects Firefox ESR < 60.2.2 and Firefox < 62.0.3.
CVE-2018-12389	** 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-2018-12390	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-12392	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-12393	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-12395	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-12396	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-12397	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-12599	In ImageMagick 7.0.8-3 Q16, ReadBMPImage and WriteBMPImage in coders/bmp.c allow attackers to cause an out of bounds write via a crafted file.
CVE-2018-12600	In ImageMagick 7.0.8-3 Q16, ReadDIBImage and WriteDIBImage in coders/dib.c allow attackers to cause an out of bounds write via a crafted file.
CVE-2018-12617	qmp_guest_file_read in qga/commands-posix.c and qga/commands-win32.c in qemu-ga (aka QEMU Guest Agent) in QEMU 2.12.50 has an integer overflow causing a g_malloc0() call to trigger a segmentation fault when trying to allocate a large memory chunk. The vulnerability can be exploited by sending a crafted QMP

	command (including guest-file-read with a large count value) to the agent via the listening socket.
CVE-2018-12824	Adobe Flash Player 30.0.0.134 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-12825	Adobe Flash Player 30.0.0.134 and earlier have a security bypass vulnerability. Successful exploitation could lead to security mitigation bypass.
CVE-2018-12826	Adobe Flash Player 30.0.0.134 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-12827	Adobe Flash Player 30.0.0.134 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-12828	Adobe Flash Player 30.0.0.134 and earlier have a "use of a component with a known vulnerability" vulnerability. Successful exploitation could lead to privilege escalation.
CVE-2018-1283	In Apache httpd 2.4.0 to 2.4.29, when mod_session is configured to forward its session data to CGI applications (SessionEnv on, not the default), a remote user may influence their content by using a "Session" header. This comes from the "HTTP_SESSION" variable name used by mod_session to forward its data to CGIs, since the prefix "HTTP_" is also used by the Apache HTTP Server to pass HTTP header fields, per CGI specifications.
CVE-2018-12904	In arch/x86/kvm/vmx.c in the Linux kernel before 4.17.2, when nested virtualization is used, local attackers could cause L1 KVM guests to VMEXIT, potentially allowing privilege escalations and denial of service attacks due to lack of checking of CPL.
CVE-2018-12910	The get_cookies function in soup-cookie-jar.c in libsoup 2.63.2 allows attackers to have unspecified impact via an empty hostname.
CVE-2018-12911	WebKitGTK+ 2.20.3 has an off-by-one error, with a resultant out-of-bounds write, in the get_simple_globs functions in ThirdParty/xdgmime/src/xdgmimecache.c and ThirdParty/xdgmime/src/xdgmimeglob.c.
CVE-2018-1301	A specially crafted request could have crashed the Apache HTTP Server prior to version 2.4.30, due to an out of bound access after a size limit is reached by reading the HTTP header. This vulnerability is considered very hard if not impossible to trigger in non-debug mode (both log and build level), so it is classified as low risk for common server usage.
CVE-2018-1303	A specially crafted HTTP request header could have crashed the Apache HTTP Server prior to version 2.4.30 due to an out of bound read while preparing

	data to be cached in shared memory. It could be used as a Denial of Service attack against users of mod_cache_socache. The vulnerability is considered as low risk since mod_cache_socache is not widely used, mod_cache_disk is not concerned by this vulnerability.
CVE-2018-1304	The URL pattern of "" (the empty string) which exactly maps to the context root was not correctly handled in Apache Tomcat 9.0.0.M1 to 9.0.4, 8.5.0 to 8.5.27, 8.0.0.RC1 to 8.0.49 and 7.0.0 to 7.0.84 when used as part of a security constraint definition. This caused the constraint to be ignored. It was, therefore, possible for unauthorised users to gain access to web application resources that should have been protected. Only security constraints with a URL pattern of the empty string were affected.
CVE-2018-1305	Security constraints defined by annotations of Servlets in Apache Tomcat 9.0.0.M1 to 9.0.4, 8.5.0 to 8.5.27, 8.0.0.RC1 to 8.0.49 and 7.0.0 to 7.0.84 were only applied once a Servlet had been loaded. Because security constraints defined in this way apply to the URL pattern and any URLs below that point, it was possible - depending on the order Servlets were loaded - for some security constraints not to be applied. This could have exposed resources to users who were not authorised to access them.
CVE-2018-13094	An issue was discovered in fs/xfs/libxfs/xfs_attr_leaf.c in the Linux kernel through 4.17.3. An OOPS may occur for a corrupted xfs image after xfs_da_shrink_inode() is called with a NULL bp.
CVE-2018-1312	In Apache httpd 2.2.0 to 2.4.29, when generating an HTTP Digest authentication challenge, the nonce sent to prevent reply attacks was not correctly generated using a pseudo-random seed. In a cluster of servers using a common Digest authentication configuration, HTTP requests could be replayed across servers by an attacker without detection.
CVE-2018-13153	In ImageMagick 7.0.8-4, there is a memory leak in the XMagickCommand function in MagickCore/animate.c.
CVE-2018-13259	An issue was discovered in zsh before 5.6. Shebang lines exceeding 64 characters were truncated, potentially leading to an execve call to a program name that is a substring of the intended one.
CVE-2018-1336	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-2018-13405	The inode_init_owner function in fs/inode.c in the Linux kernel through 4.17.4 allows local users to

	create files with an unintended group ownership, in a scenario where a directory is SGID to a certain group and is writable by a user who is not a member of that group. Here, the non-member can trigger creation of a plain file whose group ownership is that group. The intended behavior was that the non-member can trigger creation of a directory (but not a plain file) whose group ownership is that group. The non-member can escalate privileges by making the plain file executable and SGID.
CVE-2018-13406	An integer overflow in the uvesafb_setcmap function in drivers/video/fbdev/uvesafb.c in the Linux kernel before 4.17.4 could result in local attackers being able to crash the kernel or potentially elevate privileges because kmalloc_array is not used.
CVE-2018-13785	In libpng 1.6.34, a wrong calculation of row_factor in the png_check_chunk_length function (pngrutil.c) may trigger an integer overflow and resultant divide-by-zero while processing a crafted PNG file, leading to a denial of service.
CVE-2018-13988	Poppler through 0.62 contains an out of bounds read vulnerability due to an incorrect memory access that is not mapped in its memory space, as demonstrated by pdfunite. This can result in memory corruption and denial of service. This may be exploitable when a victim opens a specially crafted PDF file.
CVE-2018-14349	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap/command.c mishandles a NO response without a message.
CVE-2018-14350	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap/message.c has a stack-based buffer overflow for a FETCH response with a long INTERNALDATE field.
CVE-2018-14351	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap/command.c mishandles a long IMAP status mailbox literal count size.
CVE-2018-14352	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap_quote_string in imap/util.c does not leave room for quote characters, leading to a stack-based buffer overflow.
CVE-2018-14353	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap_quote_string in imap/util.c has an integer underflow.
CVE-2018-14354	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. They allow remote IMAP servers to execute arbitrary commands via backquote characters, related to the mailboxes command associated with a manual subscription or unsubscription.

CVE-2018-14355	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap/util.c mishandles ".." directory traversal in a mailbox name.
CVE-2018-14356	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. pop.c mishandles a zero-length UID.
CVE-2018-14357	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. They allow remote IMAP servers to execute arbitrary commands via backquote characters, related to the mailboxes command associated with an automatic subscription.
CVE-2018-14358	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. imap/message.c has a stack-based buffer overflow for a FETCH response with a long RFC822.SIZE field.
CVE-2018-14359	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. They have a buffer overflow via base64 data.
CVE-2018-14362	An issue was discovered in Mutt before 1.10.1 and NeoMutt before 2018-07-16. pop.c does not forbid characters that may have unsafe interaction with message-cache pathnames, as demonstrated by a '/' character.
CVE-2018-14404	A NULL pointer dereference vulnerability exists in the xpath.c:xmlXPathCompOpEval() function of libxml2 through 2.9.8 when parsing an invalid XPath expression in the XPATH_OP_AND or XPATH_OP_OR case. Applications processing untrusted XSL format inputs with the use of the libxml2 library may be vulnerable to a denial of service attack due to a crash of the application.
CVE-2018-14434	ImageMagick 7.0.8-4 has a memory leak for a colormap in WriteMPCImage in coders/mpc.c.
CVE-2018-14435	ImageMagick 7.0.8-4 has a memory leak in DecodeImage in coders/pcd.c.
CVE-2018-14436	ImageMagick 7.0.8-4 has a memory leak in ReadMIFFImage in coders/miff.c.
CVE-2018-14437	ImageMagick 7.0.8-4 has a memory leak in parse8BIM in coders/meta.c.
CVE-2018-14526	An issue was discovered in rsn_supp/wpa.c in wpa_supplicant 2.0 through 2.6. Under certain conditions, the integrity of EAPOL-Key messages is not checked, leading to a decryption oracle. An attacker within range of the Access Point and client can abuse the vulnerability to recover sensitive information.
CVE-2018-14567	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-2018-14622	A null-pointer dereference vulnerability was found in libtirpc before version 0.3.3-rc3. The return value of makefd_xprt() was not checked in all instances, which could lead to a crash when the server exhausted the maximum number of available file descriptors. A remote attacker could cause an rpc-based application to crash by flooding it with new connections.
CVE-2018-14625	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-2018-14629	A denial of service vulnerability was discovered in Samba's LDAP server before versions 4.7.12, 4.8.7, and 4.9.3. A CNAME loop could lead to infinite recursion in the server. An unprivileged local attacker could create such an entry, leading to denial of service.

CVE-2018-14633	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-2018-14647	Python's elementtree C accelerator failed to initialise Expat's hash salt during initialization. This could make it easy to conduct denial of service attacks against Expat by constructing an XML document that would cause pathological hash collisions in Expat's internal data structures, consuming large amounts CPU and RAM. Python 3.8, 3.7, 3.6, 3.5, 3.4, 2.7 are believed to be vulnerable.
CVE-2018-14665	A flaw was found in xorg-x11-server before 1.20.3. An incorrect permission check for -modulepath and -logfile options when starting Xorg. X server allows unprivileged users with the ability to log in to the system via physical console to escalate their privileges and run arbitrary code under root privileges.
CVE-2018-14679	An issue was discovered in mspack/chmd.c in libmspack before 0.7alpha. There is an off-by-one error in the CHM PMGI/PMGL chunk number validity checks, which could lead to denial of service (uninitialized data dereference and application crash).
CVE-2018-14680	An issue was discovered in mspack/chmd.c in libmspack before 0.7alpha. It does not reject blank CHM filenames.
CVE-2018-14681	An issue was discovered in kwajd_read_headers in mspack/kwajd.c in libmspack before 0.7alpha. Bad KWAJ file header extensions could cause a one or two byte overwrite.
CVE-2018-14682	An issue was discovered in mspack/chmd.c in libmspack before 0.7alpha. There is an off-by-one error in the TOLOWER() macro for CHM decompression.
CVE-2018-14734	drivers/infiniband/core/ucma.c in the Linux kernel through 4.17.11 allows ucma_leave_multicast to access a certain data structure after a cleanup step in ucma_process_join, which allows attackers to cause a denial of service (use-after-free).

CVE-2018-14851	exif_process_IFD_in_MAKERNOTE in ext/exif/exif.c in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted JPEG file.
CVE-2018-14883	An issue was discovered in PHP before 5.6.37, 7.0.x before 7.0.31, 7.1.x before 7.1.20, and 7.2.x before 7.2.8. An Integer Overflow leads to a heap-based buffer over-read in exif_thumbnail_extract of exif.c.
CVE-2018-15126	LibVNC before commit 73cb96fec028a576a5a24417b57723b55854ad7b contains heap use-after-free vulnerability in server code of file transfer extension that can result remote code execution
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-2018-15378	A vulnerability in ClamAV versions prior to 0.100.2 could allow an attacker to cause a denial of service (DoS) condition. The vulnerability is due to an error related to the MEW unpacker within the "unmew11()" function (libclamav/mew.c), which can be exploited to trigger an invalid read memory access via a specially crafted EXE file.
CVE-2018-15471	An issue was discovered in xenvif_set_hash_mapping in drivers/net/xen-netback/hash.c in the Linux kernel through 4.18.1, as used in Xen through 4.11.x and other products. The Linux netback driver allows frontends to control mapping of requests to request queues. When processing a request to set or change this mapping, some input validation (e.g., for an integer overflow) was missing or flawed, leading to OOB access in hash handling. A malicious or buggy frontend may cause the (usually privileged) backend to make out of bounds memory accesses, potentially resulting in one or more of privilege escalation, Denial of Service (DoS), or information leaks.
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-2018-15572	The spectre_v2_select_mitigation function in arch/x86/kernel/cpu/bugs.c in the Linux kernel before 4.18.1 does not always fill RSB upon a context switch, which makes it easier for attackers to conduct userspace-userspace spectreRSB attacks.

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-2018-15686	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-2018-15687	A race condition in chown_one() of systemd allows an attacker to cause systemd to set arbitrary permissions on arbitrary files. Affected releases are systemd versions up to and including 239.
CVE-2018-15688	A buffer overflow vulnerability in the dhcp6 client of systemd allows a malicious dhcp6 server to overwrite heap memory in systemd-networkd. Affected releases are systemd: versions up to and including 239.
CVE-2018-15853	Endless recursion exists in xkbcomp/expr.c in xkbcommon and libxkbcommon before 0.8.1, which could be used by local attackers to crash xkbcommon users by supplying a crafted keymap file that triggers boolean negation.
CVE-2018-15854	Unchecked NULL pointer usage in xkbcommon before 0.8.1 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file, because geometry tokens were desupported incorrectly.
CVE-2018-15855	Unchecked NULL pointer usage in xkbcommon before 0.8.1 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file, because the XkbFile for an xkb_geometry section was mishandled.
CVE-2018-15856	An infinite loop when reaching EOL unexpectedly in compose/parser.c (aka the keymap parser) in xkbcommon before 0.8.1 could be used by local attackers to cause a denial of service during parsing of crafted keymap files.
CVE-2018-15857	An invalid free in ExprAppendMultiKeysymList in xkbcomp/ast-build.c in xkbcommon before 0.8.1 could be used by local attackers to crash xkbcommon keymap parsers or possibly have unspecified other impact by supplying a crafted keymap file.
CVE-2018-15858	Unchecked NULL pointer usage when handling invalid aliases in CopyKeyAliasesToKeymap in xkbcomp/keycodes.c in xkbcommon before 0.8.1 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file.

CVE-2018-15859	Unchecked NULL pointer usage when parsing invalid atoms in ExprResolveLhs in xkbcomp/expr.c in xkbcommon before 0.8.2 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file, because lookup failures are mishandled.
CVE-2018-15861	Unchecked NULL pointer usage in ExprResolveLhs in xkbcomp/expr.c in xkbcommon before 0.8.2 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file that triggers an xkb_intern_atom failure.
CVE-2018-15862	Unchecked NULL pointer usage in LookupModMask in xkbcomp/expr.c in xkbcommon before 0.8.2 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file with invalid virtual modifiers.
CVE-2018-15863	Unchecked NULL pointer usage in ResolveStateAndPredicate in xkbcomp/compat.c in xkbcommon before 0.8.2 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file with a no-op modmask expression.
CVE-2018-15864	Unchecked NULL pointer usage in resolve_keysym in xkbcomp/parser.y in xkbcommon before 0.8.2 could be used by local attackers to crash (NULL pointer dereference) the xkbcommon parser by supplying a crafted keymap file, because a map access attempt can occur for a map that was never created.
CVE-2018-15908	In Artifex Ghostscript 9.23 before 2018-08-23, attackers are able to supply malicious PostScript files to bypass .tempfile restrictions and write files.
CVE-2018-15909	In Artifex Ghostscript 9.23 before 2018-08-24, a type confusion using the .shfill operator could be used by attackers able to supply crafted PostScript files to crash the interpreter or potentially execute code.
CVE-2018-15910	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files could use a type confusion in the LockDistillerParams parameter to crash the interpreter or execute code.
CVE-2018-15911	In Artifex Ghostscript 9.23 before 2018-08-24, attackers able to supply crafted PostScript could use uninitialized memory access in the aesdecode operator to crash the interpreter or potentially execute code.
CVE-2018-15967	Adobe Flash Player versions 30.0.0.154 and earlier have a privilege escalation vulnerability. Successful exploitation could lead to information disclosure.

CVE-2018-15978	Flash Player versions 31.0.0.122 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-15981	Flash Player versions 31.0.0.148 and earlier have a type confusion vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2018-15982	Flash Player versions 31.0.0.153 and earlier, and 31.0.0.108 and earlier have a use after free vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2018-15983	Flash Player versions 31.0.0.153 and earlier, and 31.0.0.108 and earlier have an insecure library loading (dll hijacking) vulnerability. Successful exploitation could lead to privilege escalation.
CVE-2018-16065	A Javascript reentrancy issues that caused a use-after-free in V8 in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-16066	A use after free in Blink in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-16067	A use after free in WebAudio in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-16068	Missing validation in Mojo in Google Chrome prior to 69.0.3497.81 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page.
CVE-2018-16069	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16070	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16071	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	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16074	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the

	candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16075	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16076	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	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-16078	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-2018-16140	A buffer underwrite vulnerability in get_line() (read.c) in fig2dev 3.2.7a allows an attacker to write prior to the beginning of the buffer via a crafted .fig file.
CVE-2018-16151	In verify_emsa_pkcs1_signature() in gmp_rsa_public_key.c in the gmp plugin in strongSwan 4.x and 5.x before 5.7.0, the RSA implementation based on GMP does not reject excess data after the encoded algorithm OID during PKCS#1 v1.5 signature verification. Similar to the flaw in the same version of strongSwan regarding digestAlgorithm.parameters, a remote attacker can forge signatures when small public exponents are being used, which could lead to impersonation when only an RSA signature is used for IKEv2 authentication.
CVE-2018-16152	In verify_emsa_pkcs1_signature() in gmp_rsa_public_key.c in the gmp plugin in strongSwan 4.x and 5.x before 5.7.0, the RSA implementation based on GMP does not reject excess data in the digestAlgorithm.parameters field during PKCS#1 v1.5 signature verification. Consequently, a remote attacker can forge signatures when small public exponents are being used, which could lead to impersonation when only an RSA signature is used for IKEv2 authentication. This is a variant of CVE-2006-4790 and CVE-2014-1568.
CVE-2018-16276	An issue was discovered in yurex_read in drivers/usb/misc/yurex.c in the Linux kernel before 4.17.7. Local attackers could use user access read/writes with incorrect bounds checking in the yurex USB driver to crash the kernel or potentially escalate privileges.
CVE-2018-16323	ReadXBMImage in coders/xbm.c in ImageMagick before 7.0.8-9 leaves data uninitialized when processing an XBM file that has a negative pixel value. If the affected code is used as a library loaded into a process that includes sensitive information, that information sometimes can be leaked via the image data.
CVE-2018-16336	Exiv2::Internal::PngChunk::parseTXTChunk in Exiv2 v0.26 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted image file, a different vulnerability than CVE-2018-10999.
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-2018-16428	In GNOME GLib 2.56.1, g_markup_parse_context_end_parse() in gmarkup.c has a NULL pointer dereference.
CVE-2018-16429	GNOME GLib 2.56.1 has an out-of-bounds read vulnerability in g_markup_parse_context_parse() in gmarkup.c, related to utf8_str().
CVE-2018-16435	Little CMS (aka Little Color Management System) 2.9 has an integer overflow in the AllocateDataSet function in cmscgats.c, leading to a heap-based buffer overflow in the SetData function via a crafted file in the second argument to cmsIT8LoadFromFile.
CVE-2018-16509	An issue was discovered in Artifex Ghostscript before 9.24. Incorrect "restoration of privilege" checking during handling of /invalidaccess exceptions could be used by attackers able to supply crafted PostScript to execute code using the "pipe" instruction.
CVE-2018-16510	An issue was discovered in Artifex Ghostscript before 9.24. Incorrect exec stack handling in the "CS" and "SC" PDF primitives could be used by remote attackers able to supply crafted PDFs to crash the interpreter or possibly have unspecified other impact.
CVE-2018-16511	An issue was discovered in Artifex Ghostscript before 9.24. A type confusion in "ztype" could be used by remote attackers able to supply crafted PostScript to crash the interpreter or possibly have unspecified other impact.
CVE-2018-16513	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files could use a type confusion in the setcolor function to crash the interpreter or possibly have unspecified other impact.
CVE-2018-16539	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files could use incorrect access checking in temp file handling to disclose contents of files on the system otherwise not readable.
CVE-2018-16540	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files to the builtin PDF14

	converter could use a use-after-free in copydevice handling to crash the interpreter or possibly have unspecified other impact.
CVE-2018-16541	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files could use incorrect free logic in pagedevice replacement to crash the interpreter.
CVE-2018-16542	In Artifex Ghostscript before 9.24, attackers able to supply crafted PostScript files could use insufficient interpreter stack-size checking during error handling to crash the interpreter.
CVE-2018-16543	In Artifex Ghostscript before 9.24, gssetresolution and gsgetresolution allow attackers to have an unspecified impact.
CVE-2018-16585	An issue was discovered in Artifex Ghostscript before 9.24. The .setdistillerkeys PostScript command is accepted even though it is not intended for use during document processing (e.g., after the startup phase). This leads to memory corruption, allowing remote attackers able to supply crafted PostScript to crash the interpreter or possibly have unspecified other impact.
CVE-2018-16640	ImageMagick 7.0.8-5 has a memory leak vulnerability in the function ReadOneJNGImage in coders/png.c.
CVE-2018-16642	The function InsertRow in coders/cut.c in ImageMagick 7.0.7-37 allows remote attackers to cause a denial of service via a crafted image file due to an out-of-bounds write.
CVE-2018-16643	The functions ReadDCMImage in coders/dcm.c, ReadPWPImage in coders/pwp.c, ReadCALSImage in coders/cals.c, and ReadPICTImage in coders/pict.c in ImageMagick 7.0.8-4 do not check the return value of the fputc function, which allows remote attackers to cause a denial of service via a crafted image file.
CVE-2018-16644	There is a missing check for length in the functions ReadDCMImage of coders/dcm.c and ReadPICTImage of coders/pict.c in ImageMagick 7.0.8-11, which allows remote attackers to cause a denial of service via a crafted image.
CVE-2018-16645	There is an excessive memory allocation issue in the functions ReadBMPImage of coders/bmp.c and ReadDIBImage of coders/dib.c in ImageMagick 7.0.8-11, which allows remote attackers to cause a denial of service via a crafted image file.
CVE-2018-16646	In Poppler 0.68.0, the Parser::getObj() function in Parser.cc may cause infinite recursion via a crafted file. A remote attacker can leverage this for a DoS attack.
CVE-2018-16658	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-2018-16839	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-2018-16841	Samba from version 4.3.0 and before versions 4.7.12, 4.8.7 and 4.9.3 are vulnerable to a denial of service. When configured to accept smart-card authentication, Samba's KDC will call talloc_free() twice on the same memory if the principal in a validly signed certificate does not match the principal in the AS-REQ. This is only possible after authentication with a trusted certificate. talloc is robust against further corruption from a double-free with talloc_free() and directly calls abort(), terminating the KDC process.
CVE-2018-16842	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-2018-16843	nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive memory consumption. This issue affects nginx compiled with the ngx_http_v2_module (not compiled by default) if the 'http2' option of the 'listen' directive is used in a configuration file.
CVE-2018-16844	nginx before versions 1.15.6 and 1.14.1 has a vulnerability in the implementation of HTTP/2 that can allow for excessive CPU usage. This issue affects nginx compiled with the ngx_http_v2_module (not compiled

	by default) if the 'http2' option of the 'listen' directive is used in a configuration file.
CVE-2018-16845	nginx before versions 1.15.6, 1.14.1 has a vulnerability in the ngx_http_mp4_module, which might allow an attacker to cause infinite loop in a worker process, cause a worker process crash, or might result in worker process memory disclosure by using a specially crafted mp4 file. The issue only affects nginx if it is built with the ngx_http_mp4_module (the module is not built by default) and the .mp4. directive is used in the configuration file. Further, the attack is only possible if an attacker is able to trigger processing of a specially crafted mp4 file with the ngx_http_mp4_module.
CVE-2018-16851	Samba from version 4.0.0 and before versions 4.7.12, 4.8.7, 4.9.3 is vulnerable to a denial of service. During the processing of an LDAP search before Samba's AD DC returns the LDAP entries to the client, the entries are cached in a single memory object with a maximum size of 256MB. When this size is reached, the Samba process providing the LDAP service will follow the NULL pointer, terminating the process. There is no further vulnerability associated with this issue, merely a denial of service.
CVE-2018-16864	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-2018-16882	A use-after-free issue was found in the way the Linux kernel's KVM hypervisor processed posted interrupts when nested(=1) virtualization is enabled. In nested_get_vmcs12_pages(), in case of an error while processing posted interrupt address, it unmaps the 'pi_desc_page' without resetting 'pi_desc' descriptor address, which is later used in pi_test_and_clear_on(). A guest user/process could use this flaw to crash

	the host kernel resulting in DoS or potentially gain privileged access to a system. Kernel versions before 4.14.91 and before 4.19.13 are vulnerable.
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-2018-17204	An issue was discovered in Open vSwitch (OvS) 2.7.x through 2.7.6, affecting parse_group_prop_ntr_selection_method in lib/ofp-util.c. When decoding a group mod, it validates the group type and command after the whole group mod has been decoded. The OF1.5 decoder, however, tries to use the type and command earlier, when it might still be invalid. This causes an assertion failure (via OVS_NOT_REACHED). ovs-vswitchd does not enable support for OpenFlow 1.5 by default.
CVE-2018-17206	An issue was discovered in Open vSwitch (OvS) 2.7.x through 2.7.6. The decode_bundle function inside lib/ofp-actions.c is affected by a buffer over-read issue during BUNDLE action decoding.
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-2018-17480	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-2018-17540	The gmp plugin in strongSwan before 5.7.1 has a Buffer Overflow via a crafted certificate.
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-2018-17958	Qemu has a Buffer Overflow in rtl8139_do_receive in hw/net/rtl8139.c because an incorrect integer data type is used.
CVE-2018-17961	Artifex Ghostscript 9.25 and earlier allows attackers to bypass a sandbox protection mechanism via vectors involving errorhandler setup. NOTE: this issue exists because of an incomplete fix for CVE-2018-17183.
CVE-2018-17962	Qemu has a Buffer Overflow in pcnet_receive in hw/net/pcnet.c because an incorrect integer data type is used.
CVE-2018-17963	qemu_deliver_packet_iov in net/net.c in Qemu accepts packet sizes greater than INT_MAX, which allows attackers to cause a denial of service or possibly have unspecified other impact.
CVE-2018-18065	_set_key in agent/helpers/table_container.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an authenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.
CVE-2018-18073	Artifex Ghostscript allows attackers to bypass a sandbox protection mechanism by leveraging exposure of system operators in the saved execution stack in an error object.
CVE-2018-18074	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-2018-18281	Since Linux kernel version 3.2, the mremap() syscall performs TLB flushes after dropping pagetable locks. If a syscall such as ftruncate() removes entries from the pagetables of a task that is in the middle of mremap(), a stale TLB entry can remain for a short time that permits access to a physical page after it has been released back to the page allocator and reused. This is fixed in the following kernel versions: 4.9.135, 4.14.78, 4.18.16, 4.19.
CVE-2018-18284	Artifex Ghostscript 9.25 and earlier allows attackers to bypass a sandbox protection mechanism via vectors involving the 1Policy operator.
CVE-2018-18311	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-2018-18312	Perl before 5.26.3 and 5.28.0 before 5.28.1 has a buffer overflow via a crafted regular expression that triggers invalid write operations.
CVE-2018-18313	Perl before 5.26.3 has a buffer over-read via a crafted regular expression that triggers disclosure of sensitive information from process memory.
CVE-2018-18314	Perl before 5.26.3 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-2018-18445	In the Linux kernel 4.14.x, 4.15.x, 4.16.x, 4.17.x, and 4.18.x before 4.18.13, faulty computation of numeric bounds in the BPF verifier permits out-of-bounds memory accesses because adjust_scalar_min_max_vals in kernel/bpf/verifier.c mishandles 32-bit right shifts.
CVE-2018-18500	A use-after-free vulnerability can occur while parsing an HTML5 stream in concert with custom HTML elements. This results in the stream parser object being freed while still in use, leading to a potentially exploitable crash. This vulnerability affects Thunderbird < 60.5, Firefox ESR < 60.5, and Firefox < 65.

CVE-2018-18501	Mozilla developers and community members reported memory safety bugs present in Firefox 64 and Firefox ESR 60.4. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 60.5, Firefox ESR < 60.5, and Firefox < 65.
CVE-2018-18502	Mozilla developers and community members reported memory safety bugs present in Firefox 64. 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 < 65.
CVE-2018-18503	When JavaScript is used to create and manipulate an audio buffer, a potentially exploitable crash may occur because of a compartment mismatch in some situations. This vulnerability affects Firefox < 65.
CVE-2018-18504	A crash and out-of-bounds read can occur when the buffer of a texture client is freed while it is still in use during graphic operations. This results is a potentially exploitable crash and the possibility of reading from the memory of the freed buffers. This vulnerability affects Firefox < 65.
CVE-2018-18505	An earlier fix for an Inter-process Communication (IPC) vulnerability, CVE-2011-3079, added authentication to communication between IPC endpoints and server parents during IPC process creation. This authentication is insufficient for channels created after the IPC process is started, leading to the authentication not being correctly applied to later channels. This could allow for a sandbox escape through IPC channels due to lack of message validation in the listener process. This vulnerability affects Thunderbird < 60.5, Firefox ESR < 60.5, and Firefox < 65.
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-2018-18557	LibTIFF 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-2018-18751	An issue was discovered in GNU gettext 0.19.8. There is a double free in default_add_message in read-catalog.c, related to an invalid free in po_gram_parse in po-gram-gen.y, as demonstrated by lt-msgfmt.
CVE-2018-18849	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-18955	In the Linux kernel 4.15.x through 4.19.x before 4.19.2, map_write() in kernel/user_namespace.c allows privilege escalation because it mishandles nested user namespaces with more than 5 UID or GID ranges. A user who has CAP_SYS_ADMIN in an affected user namespace can bypass access controls on resources outside the namespace, as demonstrated by reading /etc/shadow. This occurs because an ID transformation takes place properly for the namespaced-to-kernel direction but not for the kernel-to-namespaced direction.
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-2018-19149	Poppler before 0.70.0 has a NULL pointer dereference in _poppler_attachment_new when called from poppler_annot_file_attachment_get_attachment.
CVE-2018-19364	hw/9pfs/cofile.c and hw/9pfs/9p.c in QEMU can modify an fid path while it is being accessed by a second thread, leading to (for example) a use-after-free outcome.

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-2018-19787	An issue was discovered in lxml before 4.2.5. lxml/html/clean.py in the lxml.html.clean module does not remove javascript: URLs that use escaping, allowing a remote attacker to conduct XSS attacks, as demonstrated by "j a v a s c r i p t:" in Internet Explorer. This is a similar issue to CVE-2014-3146.
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-2018-19840	The function WavpackPackInit in pack_utils.c in libwavpack.a in WavPack through 5.1.0 allows attackers to cause a denial-of-service (resource exhaustion caused by an infinite loop) via a crafted wav audio file because WavpackSetConfiguration64 mishandles a sample rate of zero.
CVE-2018-19841	The function WavpackVerifySingleBlock in open_utils.c in libwavpack.a in WavPack through 5.1.0 allows attackers to cause a denial-of-service (out-of-bounds read and application crash) via a crafted WavPack Lossless Audio file, as demonstrated by wvunpack.
CVE-2018-20019	LibVNC before commit a83439b9fbe0f03c48eb94ed05729cb016f8b72f contains multiple heap out-of-bound write vulnerabilities in VNC client code that can result remote code execution
CVE-2018-20020	LibVNC before commit 7b1ef0ffc4815cab9a96c7278394152bdc89dc4d contains heap out-of-bound write vulnerability inside structure in VNC client code that can result remote code execution

CVE-2018-20021	LibVNC before commit c3115350eb8bb635d0fdb4dbbb0d0541f38ed19c contains a CWE-835: Infinite loop vulnerability in VNC client code. Vulnerability allows attacker to consume excessive amount of resources like CPU and RAM
CVE-2018-20022	LibVNC before 2f5b2ad1c6c99b1ac6482c95844a84d66bb52838 contains multiple weaknesses CWE-665: Improper Initialization vulnerability in VNC client code that allows attacker to read stack memory and can be abuse for information disclosure. Combined with another vulnerability, it can be used to leak stack memory layout and in bypassing ASLR
CVE-2018-20023	LibVNC before 8b06f835e259652b0ff026898014fc7297ade858 contains CWE-665: Improper Initialization vulnerability in VNC Repeater client code that allows attacker to read stack memory and can be abuse for information disclosure. Combined with another vulnerability, it can be used to leak stack memory layout and in bypassing ASLR
CVE-2018-20024	LibVNC before commit 4a21bbd097ef7c44bb000c3bd0907f96a10e4ce7 contains null pointer dereference in VNC client code that can result DoS.
CVE-2018-20102	An out-of-bounds read in dns_validate_dns_response in dns.c was discovered in HAProxy through 1.8.14. Due to a missing check when validating DNS responses, remote attackers might be able read the 16 bytes corresponding to an AAAA record from the non-initialized part of the buffer, possibly accessing anything that was left on the stack, or even past the end of the 8193-byte buffer, depending on the value of accepted_payload_size.
CVE-2018-20459	In radare2 through 3.1.3, the armass_assemble function in libr/asm/arch/arm/armass.c allows attackers to cause a denial-of-service (application crash by out-of-bounds read) by crafting an arm assembly input because a loop uses an incorrect index in armass.c and certain length validation is missing in armass64.c, a related issue to CVE-2018-20457.
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-2018-20544	There is floating point exception at caca/dither.c (function caca_dither_bitmap) in libcaca 0.99.beta19.

CVE-2018-20545	There is an illegal WRITE memory access at common-image.c (function load_image) in libcaca 0.99.beta19 for 4bpp data.
CVE-2018-20546	There is an illegal READ memory access at caca/dither.c (function get_rgba_default) in libcaca 0.99.beta19 for the default bpp case.
CVE-2018-20547	There is an illegal READ memory access at caca/dither.c (function get_rgba_default) in libcaca 0.99.beta19 for 24bpp data.
CVE-2018-20548	There is an illegal WRITE memory access at common-image.c (function load_image) in libcaca 0.99.beta19 for 1bpp data.
CVE-2018-20549	There is an illegal WRITE memory access at caca/file.c (function caca_file_read) in libcaca 0.99.beta19.
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-2018-20685	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-2018-20748	LibVNC before 0.9.12 contains multiple heap out-of-bounds write vulnerabilities in libvncclient/rfbproto.c. The fix for CVE-2018-20019 was incomplete.
CVE-2018-20749	LibVNC before 0.9.12 contains a heap out-of-bounds write vulnerability in libvncserver/rfbserver.c. The fix for CVE-2018-15127 was incomplete.
CVE-2018-20750	LibVNC through 0.9.12 contains a heap out-of-bounds write vulnerability in libvncserver/rfbserver.c. The fix for CVE-2018-15127 was incomplete.
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-2018-2565	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported

	versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2573	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: GIS). Supported versions that are affected are 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-2018-2576	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2579	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-2018-2583	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Stored Procedure). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).
CVE-2018-2586	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2588	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-2018-2590	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2599	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-2018-2600	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.20 and prior.

	Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2602	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 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).
CVE-2018-2603	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).
CVE-2018-2612	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H).
CVE-2018-2618	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 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 5.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).
CVE-2018-2622	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 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).
CVE-2018-2634	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).
CVE-2018-2637	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 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-2018-2645	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).
CVE-2018-2646	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2647	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability

	can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-2663	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-2018-2667	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 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-2018-2668	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-2018-2696	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2703	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 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-2018-2755	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2018-2758	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL

	Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2759	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2761	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2762	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2766	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2767	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption).

	Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).
CVE-2018-2769	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Pluggable Auth). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2771	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Locking). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2773	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2775	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of

	MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2776	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Group Replication GCS). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via XCom to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2777	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2778	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2779	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2780	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows low privileged

	attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2781	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2782	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2783	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, 7u161 and 8u152; Java SE Embedded: 8u152; JRockit: R28.3.17. 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 complete access to all Java SE, Java SE Embedded, JRockit accessible data. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 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-2018-2784	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2786	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-2787	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-2790	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 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-2018-2796	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).
CVE-2018-2797	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 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-2018-2810	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise

	MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2812	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-2813	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).
CVE-2018-2814	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. 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-2018-2816	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2817	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2818	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this

	vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2819	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2839	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2846	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2952	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Concurrency). Supported versions that are affected are Java SE: 6u191, 7u181, 8u172 and 10.0.1; Java SE Embedded: 8u171; JRockit: R28.3.18. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: Applies to client and server deployment of Java. This vulnerability can be exploited through sandboxed Java

	Web Start applications and sandboxed Java applets. It can also be exploited by supplying data to APIs in the specified Component without using sandboxed Java Web Start applications or sandboxed Java applets, such as through a web service. CVSS 3.0 Base Score 3.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:L).
CVE-2018-3054	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3056	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).
CVE-2018-3058	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: MyISAM). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2018-3060	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS

	Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H).
CVE-2018-3061	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.22 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3062	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Memcached). Supported versions that are affected are 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via memcached to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3063	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.60 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3064	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).

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

	high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3081	Vulnerability in the MySQL Client component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client as well as unauthorized update, insert or delete access to some of MySQL Client accessible data. CVSS 3.0 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-3133	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3136	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Security). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox

	for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g. code installed by an administrator). CVSS 3.0 Base Score 3.4 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:L/A:N).
CVE-2018-3139	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Networking). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE, Java SE Embedded accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g. code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:L/I:N/A:N).
CVE-2018-3143	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3144	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Audit). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).

CVE-2018-3149	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JNDI). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2018-3150	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Utility). The supported version that is affected is Java SE: 11. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE accessible data. Note: This vulnerability applies to Java deployments that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.7 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N).
CVE-2018-3155	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0

	Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).
CVE-2018-3156	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3161	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3162	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3169	Vulnerability in the Java SE, Java SE Embedded component of Oracle Java SE (subcomponent: Hotspot). Supported versions that are affected are Java SE: 7u191, 8u182 and 11; Java SE Embedded: 8u181. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in Java SE, Java SE Embedded, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g.

	code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g. code installed by an administrator). CVSS 3.0 Base Score 8.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2018-3171	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-3173	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3174	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:C/C:N/I:N/A:H).
CVE-2018-3180	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: JSSE). Supported versions that are affected are Java SE: 6u201, 7u191, 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to

	exploit vulnerability allows unauthenticated attacker with network access via SSL/TLS to compromise Java SE, Java SE Embedded, JRockit. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of Java SE, Java SE Embedded, JRockit accessible data as well as unauthorized read access to a subset of Java SE, Java SE Embedded, JRockit accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 5.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L).
CVE-2018-3183	Vulnerability in the Java SE, Java SE Embedded, JRockit component of Oracle Java SE (subcomponent: Scripting). Supported versions that are affected are Java SE: 8u182 and 11; Java SE Embedded: 8u181; JRockit: R28.3.19. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE, Java SE Embedded, JRockit. While the vulnerability is in Java SE, Java SE Embedded, JRockit, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of Java SE, Java SE Embedded, JRockit. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g. code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g. through a web service which supplies data to the APIs. CVSS 3.0 Base Score 9.0 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).
CVE-2018-3185	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable

	crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-3187	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-3200	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3214	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-2018-3247	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Merge). Supported

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

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

	analysis, aka Speculative Store Bypass (SSB), Variant 4.
CVE-2018-3640	Systems with microprocessors utilizing speculative execution and that perform speculative reads of system registers may allow unauthorized disclosure of system parameters to an attacker with local user access via a side-channel analysis, aka Rogue System Register Read (RSRE), Variant 3a.
CVE-2018-3646	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access with guest OS privilege via a terminal page fault and a side-channel analysis.
CVE-2018-3665	System software utilizing Lazy FP state restore technique on systems using Intel Core-based microprocessors may potentially allow a local process to infer data from another process through a speculative execution side channel.
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-2018-4088	An issue was discovered in certain Apple products. iOS before 11.2.5 is affected. macOS before 10.13.3 is affected. Safari before 11.0.3 is affected. iCloud before 7.3 on Windows is affected. iTunes before 12.7.3 on Windows is affected. tvOS before 11.2.5 is affected. watchOS before 4.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2018-4096	An issue was discovered in certain Apple products. iOS before 11.2.5 is affected. macOS before 10.13.3 is affected. Safari before 11.0.3 is affected. iCloud before 7.3 on Windows is affected. iTunes before 12.7.3 on Windows is affected. tvOS before 11.2.5 is affected. watchOS before 4.2.2 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service

	(memory corruption and application crash) via a crafted web site.
CVE-2018-4101	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. tvOS before 11.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2018-4113	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. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves a JavaScriptCore function in the "WebKit" component. It allows attackers to trigger an assertion failure by leveraging improper array indexing.
CVE-2018-4114	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. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2018-4117	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-2018-4118	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. tvOS before 11.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2018-4119	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. tvOS before 11.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2018-4120	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. tvOS before 11.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2018-4122	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. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2018-4125	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. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2018-4127	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. tvOS before 11.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2018-4128	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. tvOS before 11.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2018-4129	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. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.

CVE-2018-4133	An issue was discovered in certain Apple products. Safari before 11.1 is affected. The issue involves the "WebKit" component. A Safari cross-site scripting (XSS) vulnerability allows remote attackers to inject arbitrary web script or HTML via a crafted URL.
CVE-2018-4146	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. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows attackers to cause a denial of service (memory corruption) via a crafted web site.
CVE-2018-4161	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. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2018-4162	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. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2018-4163	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. tvOS before 11.3 is affected. watchOS before 4.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2018-4165	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. tvOS before 11.3 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2018-4180	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.

CVE-2018-4181	In macOS High Sierra before 10.13.5, an issue existed in CUPS. This issue was addressed with improved access restrictions.
CVE-2018-4190	An issue was discovered in certain Apple products. iOS before 11.4 is affected. Safari before 11.1.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to obtain sensitive credential information that is transmitted during a CSS mask-image fetch.
CVE-2018-4199	An issue was discovered in certain Apple products. iOS before 11.4 is affected. Safari before 11.1.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a crafted web site.
CVE-2018-4200	An issue was discovered in certain Apple products. iOS before 11.3.1 is affected. Safari before 11.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site that triggers a WebCore::jsElementScrollHeightGetter use-after-free.
CVE-2018-4218	An issue was discovered in certain Apple products. iOS before 11.4 is affected. Safari before 11.1.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4 is affected. watchOS before 4.3.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site that triggers an @generatorState use-after-free.
CVE-2018-4222	An issue was discovered in certain Apple products. iOS before 11.4 is affected. Safari before 11.1.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4 is affected. watchOS before 4.3.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code via a crafted web site that leverages a getWasmBufferFromValue out-of-bounds read during WebAssembly compilation.
CVE-2018-4232	An issue was discovered in certain Apple products. iOS before 11.4 is affected. Safari before 11.1.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4

	is affected. The issue involves the "WebKit" component. It allows remote attackers to overwrite cookies via a crafted web site.
CVE-2018-4233	An issue was discovered in certain Apple products. iOS before 11.4 is affected. Safari before 11.1.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4 is affected. watchOS before 4.3.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash) via a crafted web site.
CVE-2018-4246	An issue was discovered in certain Apple products. iOS before 11.4 is affected. Safari before 11.1.1 is affected. iCloud before 7.5 on Windows is affected. iTunes before 12.7.5 on Windows is affected. tvOS before 11.4 is affected. watchOS before 4.3.1 is affected. The issue involves the "WebKit" component. It allows remote attackers to execute arbitrary code via a crafted web site that leverages type confusion.
CVE-2018-4262	In Safari before 11.1.2, iTunes before 12.8 for Windows, iOS before 11.4.1, tvOS before 11.4.1, iCloud for Windows before 7.6, multiple memory corruption issues were addressed with improved memory handling.
CVE-2018-4278	In Safari before 11.1.2, iTunes before 12.8 for Windows, iOS before 11.4.1, tvOS before 11.4.1, iCloud for Windows before 7.6, sound fetched through audio elements may be exfiltrated cross-origin. This issue was addressed with improved audio taint tracking.
CVE-2018-4871	An Out-of-bounds Read issue was discovered in Adobe Flash Player before 28.0.0.137. This vulnerability occurs because of computation that reads data that is past the end of the target buffer. The use of an invalid (out-of-range) pointer offset during access of internal data structure fields causes the vulnerability. A successful attack can lead to sensitive data exposure.
CVE-2018-4877	A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to a dangling pointer in the Primetime SDK related to media player's quality of service functionality. A successful attack can lead to arbitrary code execution.
CVE-2018-4878	A use-after-free vulnerability was discovered in Adobe Flash Player before 28.0.0.161. This vulnerability occurs due to a dangling pointer in the Primetime SDK related to media player handling of listener objects. A successful attack can lead to arbitrary code execution. This was exploited in the wild in January and February 2018.

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

	Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-5007	Adobe Flash Player 30.0.0.113 and earlier versions have a Type Confusion vulnerability. Successful exploitation could lead to arbitrary code execution in the context of the current user.
CVE-2018-5008	Adobe Flash Player 30.0.0.113 and earlier versions have an Out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure.
CVE-2018-5089	Memory safety bugs were reported in Firefox 57 and Firefox ESR 52.5. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 52.6, Firefox ESR < 52.6, and Firefox < 58.
CVE-2018-5090	Memory safety bugs were reported in Firefox 57. 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 < 58.
CVE-2018-5091	A use-after-free vulnerability can occur during WebRTC connections when interacting with the DTMF timers. This results in a potentially exploitable crash. This vulnerability affects Firefox ESR < 52.6 and Firefox < 58.
CVE-2018-5092	A use-after-free vulnerability can occur when the thread for a Web Worker is freed from memory prematurely instead of from memory in the main thread while cancelling fetch operations. This vulnerability affects Firefox < 58.
CVE-2018-5093	A heap buffer overflow vulnerability may occur in WebAssembly during Memory/Table resizing, resulting in a potentially exploitable crash. This vulnerability affects Firefox < 58.
CVE-2018-5094	A heap buffer overflow vulnerability may occur in WebAssembly when "shrinkElements" is called followed by garbage collection on memory that is now uninitialized. This results in a potentially exploitable crash. This vulnerability affects Firefox < 58.
CVE-2018-5095	An integer overflow vulnerability in the Skia library when allocating memory for edge builders on some systems with at least 8 GB of RAM. This results in the use of uninitialized memory, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.6, Firefox ESR < 52.6, and Firefox < 58.
CVE-2018-5096	A use-after-free vulnerability can occur while editing events in form elements on a page, resulting in a

	potentially exploitable crash. This vulnerability affects Firefox ESR < 52.6 and Thunderbird < 52.6.
CVE-2018-5097	A use-after-free vulnerability can occur during XSL transformations when the source document for the transformation is manipulated by script content during the transformation. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.6, Firefox ESR < 52.6, and Firefox < 58.
CVE-2018-5098	A use-after-free vulnerability can occur when form input elements, focus, and selections are manipulated by script content. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.6, Firefox ESR < 52.6, and Firefox < 58.
CVE-2018-5099	A use-after-free vulnerability can occur when the widget listener is holding strong references to browser objects that have previously been freed, resulting in a potentially exploitable crash when these references are used. This vulnerability affects Thunderbird < 52.6, Firefox ESR < 52.6, and Firefox < 58.
CVE-2018-5100	A use-after-free vulnerability can occur when arguments passed to the "IsPotentiallyScrollable" function are freed while still in use by scripts. This results in a potentially exploitable crash. This vulnerability affects Firefox < 58.
CVE-2018-5101	A use-after-free vulnerability can occur when manipulating floating "first-letter" style elements, resulting in a potentially exploitable crash. This vulnerability affects Firefox < 58.
CVE-2018-5102	A use-after-free vulnerability can occur when manipulating HTML media elements with media streams, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.6, Firefox ESR < 52.6, and Firefox < 58.
CVE-2018-5103	A use-after-free vulnerability can occur during mouse event handling due to issues with multiprocess support. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.6, Firefox ESR < 52.6, and Firefox < 58.
CVE-2018-5104	A use-after-free vulnerability can occur during font face manipulation when a font face is freed while still in use, resulting in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.6, Firefox ESR < 52.6, and Firefox < 58.
CVE-2018-5105	WebExtensions can bypass user prompts to first save and then open an arbitrarily downloaded file. This can result in an executable file running with local user privileges without explicit user consent. This vulnerability affects Firefox < 58.

CVE-2018-5106	Style editor traffic in the Developer Tools can be routed through a service worker hosted on a third party website if a user selects error links when these tools are open. This can allow style editor information used within Developer Tools to leak cross-origin. This vulnerability affects Firefox < 58.
CVE-2018-5107	The printing process can bypass local access protections to read files available through symlinks, bypassing local file restrictions. The printing process requires files in a specific format so arbitrary data cannot be read but it is possible that some local file information could be exposed. This vulnerability affects Firefox < 58.
CVE-2018-5108	A Blob URL can violate origin attribute segregation, allowing it to be accessed from a private browsing tab and for data to be passed between the private browsing tab and a normal tab. This could allow for the leaking of private information specific to the private browsing context. This issue is mitigated by the requirement that the user enter the Blob URL manually in order for the access violation to occur. This vulnerability affects Firefox < 58.
CVE-2018-5109	An audio capture session can started under an incorrect origin from the site making the capture request. Users are still prompted to allow the request but the prompt can display the wrong origin, leading to user confusion about which site is making the request to capture an audio stream. This vulnerability affects Firefox < 58.
CVE-2018-5111	When the text of a specially formatted URL is dragged to the addressbar from page content, the displayed URL can be spoofed to show a different site than the one loaded. This allows for phishing attacks where a malicious page can spoof the identify of another site. This vulnerability affects Firefox < 58.
CVE-2018-5112	Development Tools panels of an extension are required to load URLs for the panels as relative URLs from the extension manifest file but this requirement was not enforced in all instances. This could allow the development tools panel for the extension to load a URL that it should not be able to access, including potentially privileged pages. This vulnerability affects Firefox < 58.
CVE-2018-5113	The "browser.identity.launchWebAuthFlow" function of WebExtensions is only allowed to load content over "https:" but this requirement was not properly enforced. This can potentially allow privileged pages to be loaded by the extension. This vulnerability affects Firefox < 58.
CVE-2018-5114	If an existing cookie is changed to be "HttpOnly" while a document is open, the original value remains accessible through script until that document is closed. Network

	requests correctly use the changed HttpOnly cookie. This vulnerability affects Firefox < 58.
CVE-2018-5115	If an HTTP authentication prompt is triggered by a background network request from a page or extension, it is displayed over the currently loaded foreground page. Although the prompt contains the real domain making the request, this can result in user confusion about the originating site of the authentication request and may cause users to mistakenly send private credential information to a third party site. This vulnerability affects Firefox < 58.
CVE-2018-5116	WebExtensions with the "ActiveTab" permission are able to access frames hosted within the active tab even if the frames are cross-origin. Malicious extensions can inject frames from arbitrary origins into the loaded page and then interact with them, bypassing same-origin user expectations with this permission. This vulnerability affects Firefox < 58.
CVE-2018-5117	If right-to-left text is used in the addressbar with left-to-right alignment, it is possible in some circumstances to scroll this text to spoof the displayed URL. This issue could result in the wrong URL being displayed as a location, which can mislead users to believe they are on a different site than the one loaded. This vulnerability affects Thunderbird < 52.6, Firefox ESR < 52.6, and Firefox < 58.
CVE-2018-5118	The screenshot images displayed in the Activity Stream page displayed when a new tab is opened is created from the meta tags of websites. An issue was discovered where the page could attempt to create these images through "file:" URLs from the local file system. This loading is blocked by the sandbox but could expose local data if combined with another attack that escapes sandbox protections. This vulnerability affects Firefox < 58.
CVE-2018-5119	The reader view will display cross-origin content when CORS headers are set to prohibit the loading of cross-origin content by a site. This could allow access to content that should be restricted in reader view. This vulnerability affects Firefox < 58.
CVE-2018-5122	A potential integer overflow in the "DoCrypt" function of WebCrypto was identified. If a means was found of exploiting it, it could result in an out-of-bounds write. This vulnerability affects Firefox < 58.
CVE-2018-5124	** 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-2018-5125	Memory safety bugs were reported in Firefox 58 and Firefox ESR 52.6. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 52.7, Firefox ESR < 52.7, and Firefox < 59.
CVE-2018-5126	Memory safety bugs were reported in Firefox 58. 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 < 59.
CVE-2018-5127	A buffer overflow can occur when manipulating the SVG "animatedPathSegList" through script. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.7, Firefox ESR < 52.7, and Firefox < 59.
CVE-2018-5128	A use-after-free vulnerability can occur when manipulating elements, events, and selection ranges during editor operations. This results in a potentially exploitable crash. This vulnerability affects Firefox < 59.
CVE-2018-5129	A lack of parameter validation on IPC messages results in a potential out-of-bounds write through malformed IPC messages. This can potentially allow for sandbox escape through memory corruption in the parent process. This vulnerability affects Thunderbird < 52.7, Firefox ESR < 52.7, and Firefox < 59.
CVE-2018-5130	When packets with a mismatched RTP payload type are sent in WebRTC connections, in some circumstances a potentially exploitable crash is triggered. This vulnerability affects Firefox ESR < 52.7 and Firefox < 59.
CVE-2018-5131	Under certain circumstances the "fetch()" API can return transient local copies of resources that were sent with a "no-store" or "no-cache" cache header instead of downloading a copy from the network as it should. This can result in previously stored, locally cached data of a website being accessible to users if they share a common profile while browsing. This vulnerability affects Firefox ESR < 52.7 and Firefox < 59.
CVE-2018-5132	The Find API for WebExtensions can search some privileged pages, such as "about:debugging", if these pages are open in a tab. This could allow a malicious WebExtension to search for otherwise protected data if a user has it open. This vulnerability affects Firefox < 59.
CVE-2018-5133	If the "app.support.baseURL" preference is changed by a malicious local program to contain HTML and script content, this content is not sanitized. It will be executed if a user loads "chrome://browser/content/

	preferences/in-content/preferences.xul" directly in a tab and executes a search. This stored preference is also executed whenever an EME video player plugin displays a CDM-disabled message as a notification message. This vulnerability affects Firefox < 59.
CVE-2018-5134	WebExtensions may use "view-source:" URLs to view local "file:" URL content, as well as content stored in "about:cache", bypassing restrictions that only allow WebExtensions to view specific content. This vulnerability affects Firefox < 59.
CVE-2018-5135	WebExtensions can bypass normal restrictions in some circumstances and use "browser.tabs.executeScript" to inject scripts into contexts where this should not be allowed, such as pages from other WebExtensions or unprivileged "about:" pages. This vulnerability affects Firefox < 59.
CVE-2018-5136	A shared worker created from a "data:" URL in one tab can be shared by another tab with a different origin, bypassing the same-origin policy. This vulnerability affects Firefox < 59.
CVE-2018-5137	A legacy extension's non-contentaccessible, defined resources can be loaded by an arbitrary web page through script. This script does this by using a maliciously crafted path string to reference the resources. Note: this vulnerability does not affect WebExtensions. This vulnerability affects Firefox < 59.
CVE-2018-5140	Image for moz-icons can be accessed through the "moz-icon:" protocol through script in web content even when otherwise prohibited. This could allow for information leakage of which applications are associated with specific MIME types by a malicious page. This vulnerability affects Firefox < 59.
CVE-2018-5141	A vulnerability in the notifications Push API where notifications can be sent through service workers by web content without direct user interaction. This could be used to open new tabs in a denial of service (DOS) attack or to display unwanted content from arbitrary URLs to users. This vulnerability affects Firefox < 59.
CVE-2018-5142	If Media Capture and Streams API permission is requested from documents with "data:" or "blob:" URLs, the permission notifications do not properly display the originating domain. The notification states "Unknown protocol" as the requestee, leading to user confusion about which site is asking for this permission. This vulnerability affects Firefox < 59.
CVE-2018-5143	URLs using "javascript:" have the protocol removed when pasted into the addressbar to protect users from cross-site scripting (XSS) attacks, but if a tab character is embedded in the "javascript:" URL the protocol is not removed and the script will execute. This could allow

	users to be socially engineered to run an XSS attack against themselves. This vulnerability affects Firefox < 59.
CVE-2018-5144	An integer overflow can occur during conversion of text to some Unicode character sets due to an unchecked length parameter. This vulnerability affects Firefox ESR < 52.7 and Thunderbird < 52.7.
CVE-2018-5145	Memory safety bugs were reported in Firefox ESR 52.6. 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 < 52.7 and Thunderbird < 52.7.
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-2018-5148	A use-after-free vulnerability can occur in the compositor during certain graphics operations when a raw pointer is used instead of a reference counted one. This results in a potentially exploitable crash. This vulnerability affects Firefox ESR < 52.7.3 and Firefox < 59.0.2.
CVE-2018-5150	Memory safety bugs were reported in Firefox 59, Firefox ESR 52.7, and Thunderbird 52.7. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 52.8, Thunderbird ESR < 52.8, Firefox < 60, and Firefox ESR < 52.8.
CVE-2018-5151	Memory safety bugs were reported in Firefox 59. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 60.
CVE-2018-5152	WebExtensions with the appropriate permissions can attach content scripts to Mozilla sites such as accounts.firefox.com and listen to network traffic to the site through the "webRequest" API. For example, this allows for the interception of username and an encrypted password during login to Firefox Accounts. This issue does not expose synchronization traffic directly and is limited to the process of user login to the website and the data displayed to the user once logged in. This vulnerability affects Firefox < 60.
CVE-2018-5153	If websocket data is sent with mixed text and binary in a single message, the binary data can be corrupted. This can result in an out-of-bounds read with the read memory sent to the originating server in response. This vulnerability affects Firefox < 60.

CVE-2018-5154	A use-after-free vulnerability can occur while enumerating attributes during SVG animations with clip paths. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.8, Thunderbird ESR < 52.8, Firefox < 60, and Firefox ESR < 52.8.
CVE-2018-5155	A use-after-free vulnerability can occur while adjusting layout during SVG animations with text paths. This results in a potentially exploitable crash. This vulnerability affects Thunderbird < 52.8, Thunderbird ESR < 52.8, Firefox < 60, and Firefox ESR < 52.8.
CVE-2018-5156	A vulnerability can occur when capturing a media stream when the media source type is changed as the capture is occurring. This can result in stream data being cast to the wrong type causing a potentially exploitable crash. This vulnerability affects Thunderbird < 60, Firefox ESR < 60.1, Firefox ESR < 52.9, and Firefox < 61.
CVE-2018-5157	Same-origin protections for the PDF viewer can be bypassed, allowing a malicious site to intercept messages meant for the viewer. This could allow the site to retrieve PDF files restricted to viewing by an authenticated user on a third-party website. This vulnerability affects Firefox ESR < 52.8 and Firefox < 60.
CVE-2018-5158	The PDF viewer does not sufficiently sanitize PostScript calculator functions, allowing malicious JavaScript to be injected through a crafted PDF file. This JavaScript can then be run with the permissions of the PDF viewer by its worker. This vulnerability affects Firefox ESR < 52.8 and Firefox < 60.
CVE-2018-5159	An integer overflow can occur in the Skia library due to 32-bit integer use in an array without integer overflow checks, resulting in possible out-of-bounds writes. This could lead to a potentially exploitable crash triggerable by web content. This vulnerability affects Thunderbird < 52.8, Thunderbird ESR < 52.8, Firefox < 60, and Firefox ESR < 52.8.
CVE-2018-5160	WebRTC can use a "WrappedI420Buffer" pixel buffer but the owning image object can be freed while it is still in use. This can result in the WebRTC encoder using uninitialized memory, leading to a potentially exploitable crash. This vulnerability affects Firefox < 60.
CVE-2018-5161	Crafted message headers can cause a Thunderbird process to hang on receiving the message. This vulnerability affects Thunderbird ESR < 52.8 and Thunderbird < 52.8.
CVE-2018-5162	Plaintext of decrypted emails can leak through the src attribute of remote images, or links. This vulnerability

	affects Thunderbird ESR < 52.8 and Thunderbird < 52.8.
CVE-2018-5163	If a malicious attacker has used another vulnerability to gain full control over a content process, they may be able to replace the alternate data resources stored in the JavaScript Start-up Bytecode Cache (JSBC) for other JavaScript code. If the parent process then runs this replaced code, the executed script would be run with the parent process' privileges, escaping the sandbox on content processes. This vulnerability affects Firefox < 60.
CVE-2018-5164	Content Security Policy (CSP) is not applied correctly to all parts of multipart content sent with the "multipart/x-mixed-replace" MIME type. This could allow for script to run where CSP should block it, allowing for cross-site scripting (XSS) and other attacks. This vulnerability affects Firefox < 60.
CVE-2018-5166	WebExtensions can use request redirection and a "filterReponseData" filter to bypass host permission settings to redirect network traffic and access content from a host for which they do not have explicit user permission. This vulnerability affects Firefox < 60.
CVE-2018-5167	The web console and JavaScript debugger do not sanitize all output that can be hyperlinked. Both will display "chrome:" links as active, clickable hyperlinks in their output. Web sites should not be able to directly link to internal chrome pages. Additionally, the JavaScript debugger will display "javascript:" links, which users could be tricked into clicking by malicious sites. This vulnerability affects Firefox < 60.
CVE-2018-5168	Sites can bypass security checks on permissions to install lightweight themes by manipulating the "baseURI" property of the theme element. This could allow a malicious site to install a theme without user interaction which could contain offensive or embarrassing images. This vulnerability affects Thunderbird < 52.8, Thunderbird ESR < 52.8, Firefox < 60, and Firefox ESR < 52.8.
CVE-2018-5169	If manipulated hyperlinked text with "chrome:" URL contained in it is dragged and dropped on the "home" icon, the home page can be reset to include a normally-unlinkable chrome page as one of the home page tabs. This vulnerability affects Firefox < 60.
CVE-2018-5170	It is possible to spoof the filename of an attachment and display an arbitrary attachment name. This could lead to a user opening a remote attachment which is a different file type than expected. This vulnerability affects Thunderbird ESR < 52.8 and Thunderbird < 52.8.

CVE-2018-5172	The Live Bookmarks page and the PDF viewer can run injected script content if a user pastes script from the clipboard into them while viewing RSS feeds or PDF files. This could allow a malicious site to socially engineer a user to copy and paste malicious script content that could then run with the context of either page but does not allow for privilege escalation. This vulnerability affects Firefox < 60.
CVE-2018-5173	The filename appearing in the "Downloads" panel improperly renders some Unicode characters, allowing for the file name to be spoofed. This can be used to obscure the file extension of potentially executable files from user view in the panel. Note: the dialog to open the file will show the full, correct filename and whether it is executable or not. This vulnerability affects Firefox < 60.
CVE-2018-5175	A mechanism to bypass Content Security Policy (CSP) protections on sites that have a "script-src" policy of "'strict-dynamic'". If a target website contains an HTML injection flaw an attacker could inject a reference to a copy of the "require.js" library that is part of Firefox's Developer Tools, and then use a known technique using that library to bypass the CSP restrictions on executing injected scripts. This vulnerability affects Firefox < 60.
CVE-2018-5176	The JSON Viewer displays clickable hyperlinks for strings that are parseable as URLs, including "javascript:" links. If a JSON file contains malicious JavaScript script embedded as "javascript:" links, users may be tricked into clicking and running this code in the context of the JSON Viewer. This can allow for the theft of cookies and authorization tokens which are accessible to that context. This vulnerability affects Firefox < 60.
CVE-2018-5177	A vulnerability exists in XSLT during number formatting where a negative buffer size may be allocated in some instances, leading to a buffer overflow and crash if it occurs. This vulnerability affects Firefox < 60.
CVE-2018-5178	A buffer overflow was found during UTF8 to Unicode string conversion within JavaScript with extremely large amounts of data. This vulnerability requires the use of a malicious or vulnerable legacy extension in order to occur. This vulnerability affects Thunderbird ESR < 52.8, Thunderbird < 52.8, and Firefox ESR < 52.8.
CVE-2018-5179	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-5180	A use-after-free vulnerability can occur during WebGL operations. While this results in a potentially exploitable

	crash, the vulnerability is limited because the memory is freed and reused in a brief window of time during the freeing of the same callstack. This vulnerability affects Firefox < 60.
CVE-2018-5181	If a URL using the "file:" protocol is dragged and dropped onto an open tab that is running in a different child process the tab will open a local file corresponding to the dropped URL, contrary to policy. One way to make the target tab open more reliably in a separate process is to open it with the "noopener" keyword. This vulnerability affects Firefox < 60.
CVE-2018-5182	If a text string that happens to be a filename in the operating system's native format is dragged and dropped onto the addressbar the specified local file will be opened. This is contrary to policy and is what would happen if the string were the equivalent "file:" URL. This vulnerability affects Firefox < 60.
CVE-2018-5183	Mozilla developers backported selected changes in the Skia library. These changes correct memory corruption issues including invalid buffer reads and writes during graphic operations. This vulnerability affects Thunderbird ESR < 52.8, Thunderbird < 52.8, and Firefox ESR < 52.8.
CVE-2018-5184	Using remote content in encrypted messages can lead to the disclosure of plaintext. This vulnerability affects Thunderbird ESR < 52.8 and Thunderbird < 52.8.
CVE-2018-5185	Plaintext of decrypted emails can leak through by user submitting an embedded form. This vulnerability affects Thunderbird ESR < 52.8 and Thunderbird < 52.8.
CVE-2018-5186	Memory safety bugs present in Firefox 60. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 61.
CVE-2018-5187	Memory safety bugs present in Firefox 60 and Firefox ESR 60. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 60, Firefox ESR < 60.1, and Firefox < 61.
CVE-2018-5188	Memory safety bugs present in Firefox 60, Firefox ESR 60, and Firefox ESR 52.8. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Thunderbird < 60, Thunderbird < 52.9, Firefox ESR < 60.1, Firefox ESR < 52.9, and Firefox < 61.
CVE-2018-5205	When using incomplete escape codes, Irssi before 1.0.6 may access data beyond the end of the string.

CVE-2018-5206	When the channel topic is set without specifying a sender, Irssi before 1.0.6 may dereference a NULL pointer.
CVE-2018-5207	When using an incomplete variable argument, Irssi before 1.0.6 may access data beyond the end of the string.
CVE-2018-5208	In Irssi before 1.0.6, a calculation error in the completion code could cause a heap buffer overflow when completing certain strings.
CVE-2018-5246	In ImageMagick 7.0.7-17 Q16, there are memory leaks in ReadPATTERNImage in coders/pattern.c.
CVE-2018-5247	In ImageMagick 7.0.7-17 Q16, there are memory leaks in ReadRLAImage in coders/rla.c.
CVE-2018-5248	In ImageMagick 7.0.7-17 Q16, there is a heap-based buffer over-read in coders/sixel.c in the ReadSIXELImage function, related to the sixel_decode function.
CVE-2018-5332	In the Linux kernel through 4.14.13, the rds_message_alloc_sgs() function does not validate a value that is used during DMA page allocation, leading to a heap-based out-of-bounds write (related to the rds_rdma_extra_size function in net/rds/rdma.c).
CVE-2018-5333	In the Linux kernel through 4.14.13, the rds_cmsg_atomic function in net/rds/rdma.c mishandles cases where page pinning fails or an invalid address is supplied, leading to an rds_atomic_free_op NULL pointer dereference.
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-2018-5345	A stack-based buffer overflow within GNOME gcab through 0.7.4 can be exploited by malicious attackers to cause a crash or, potentially, execute arbitrary code via a crafted .cab file.
CVE-2018-5357	ImageMagick 7.0.7-22 Q16 has memory leaks in the ReadDCMImage function in coders/dcm.c.
CVE-2018-5358	ImageMagick 7.0.7-22 Q16 has memory leaks in the EncodeImageAttributes function in coders/json.c, as demonstrated by the ReadPSDLayersInternal function in coders/psd.c.
CVE-2018-5379	The Quagga BGP daemon (bgpd) prior to version 1.2.3 can double-free memory when processing certain forms of UPDATE message, containing cluster-list and/or unknown attributes. A successful attack could cause a denial of service or potentially allow an attacker to execute arbitrary code.

CVE-2018-5380	The Quagga BGP daemon (bgpd) prior to version 1.2.3 can overrun internal BGP code-to-string conversion tables used for debug by 1 pointer value, based on input.
CVE-2018-5381	The Quagga BGP daemon (bgpd) prior to version 1.2.3 has a bug in its parsing of "Capabilities" in BGP OPEN messages, in the bgp_packet.c:bgp_capability_msg_parse function. The parser can enter an infinite loop on invalid capabilities if a Multi-Protocol capability does not have a recognized AFI/SAFI, causing a denial of service.
CVE-2018-5388	In stroke_socket.c in strongSwan before 5.6.3, a missing packet length check could allow a buffer underflow, which may lead to resource exhaustion and denial of service while reading from the socket.
CVE-2018-5390	Linux kernel versions 4.9+ can be forced to make very expensive calls to tcp_collapse_ofo_queue() and tcp_prune_ofo_queue() for every incoming packet which can lead to a denial of service.
CVE-2018-5391	The Linux kernel, versions 3.9+, is vulnerable to a denial of service attack with low rates of specially modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service condition by sending specially crafted IP fragments. Various vulnerabilities in IP fragmentation have been discovered and fixed over the years. The current vulnerability (CVE-2018-5391) became exploitable in the Linux kernel with the increase of the IP fragment reassembly queue size.
CVE-2018-5407	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-2018-5702	Transmission through 2.92 relies on X-Transmission-Session-Id (which is not a forbidden header for Fetch) for access control, which allows remote attackers to execute arbitrary RPC commands, and consequently write to arbitrary files, via POST requests to /transmission/rpc in conjunction with a DNS rebinding attack.
CVE-2018-5711	gd_gif_in.c in the GD Graphics Library (aka libgd), as used in PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1, has an integer signedness error that leads to an infinite loop via a crafted GIF file, as demonstrated by a call to the imagecreatefromgif or imagecreatefromstring

	PHP function. This is related to GetCode_ and gdImageCreateFromGifCtx.
CVE-2018-5712	An issue was discovered in PHP before 5.6.33, 7.0.x before 7.0.27, 7.1.x before 7.1.13, and 7.2.x before 7.2.1. There is Reflected XSS on the PHAR 404 error page via the URI of a request for a .phar file.
CVE-2018-5732	An out-of-bound memory access flaw was found in the way dhclient processed a DHCP response packet. A malicious DHCP server could potentially use this flaw to crash dhclient processes running on DHCP client machines via a crafted DHCP response packet.
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-2018-5748	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-2018-5764	The parse_arguments function in options.c in rsyncd in rsync before 3.1.3 does not prevent multiple --protect-args uses, which allows remote attackers to bypass an argument-sanitization protection mechanism.
CVE-2018-5784	In LibTIFF 4.0.9, there is an uncontrolled resource consumption in the TIFFSetDirectory function of tif_dir.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted tif file. This occurs because the declared number of directory entries is not validated against the actual number of directory entries.
CVE-2018-5800	An off-by-one error within the "LibRaw::kodak_ycbcr_load_raw()" function (internal/dcraw_common.cpp) in LibRaw versions prior to 0.18.7 can be exploited to cause a heap-based buffer overflow and subsequently cause a crash.

CVE-2018-5801	An error within the "LibRaw::unpack()" function (src/libraw_cxx.cpp) in LibRaw versions prior to 0.18.7 can be exploited to trigger a NULL pointer dereference.
CVE-2018-5802	An error within the "kodak_radc_load_raw()" function (internal/dcraw_common.cpp) related to the "buf" variable in LibRaw versions prior to 0.18.7 can be exploited to cause an out-of-bounds read memory access and subsequently cause a crash.
CVE-2018-5803	In the Linux Kernel before version 4.15.8, 4.14.25, 4.9.87, 4.4.121, 4.1.51, and 3.2.102, an error in the "_sctp_make_chunk()" function (net/sctp/sm_make_chunk.c) when handling SCTP packets length can be exploited to cause a kernel crash.
CVE-2018-5807	An error within the "samsung_load_raw()" function (internal/dcraw_common.cpp) in LibRaw versions prior to 0.18.9 can be exploited to cause an out-of-bounds read memory access and subsequently cause a crash.
CVE-2018-5810	An error within the "rollei_load_raw()" function (internal/dcraw_common.cpp) in LibRaw versions prior to 0.18.9 can be exploited to cause a heap-based buffer overflow and subsequently cause a crash.
CVE-2018-5811	An error within the "nikon_coolscan_load_raw()" function (internal/dcraw_common.cpp) in LibRaw versions prior to 0.18.9 can be exploited to cause an out-of-bounds read memory access and subsequently cause a crash.
CVE-2018-5812	An error within the "nikon_coolscan_load_raw()" function (internal/dcraw_common.cpp) in LibRaw versions prior to 0.18.9 can be exploited to trigger a NULL pointer dereference.
CVE-2018-5813	An error within the "parse_minolta()" function (dcraw/dcraw.c) in LibRaw versions prior to 0.18.11 can be exploited to trigger an infinite loop via a specially crafted file.
CVE-2018-5814	In the Linux Kernel before version 4.16.11, 4.14.43, 4.9.102, and 4.4.133, multiple race condition errors when handling probe, disconnect, and rebind operations can be exploited to trigger a use-after-free condition or a NULL pointer dereference by sending multiple USB over IP packets.
CVE-2018-5815	An integer overflow error within the "parse_qt()" function (internal/dcraw_common.cpp) in LibRaw versions prior to 0.18.12 can be exploited to trigger an infinite loop via a specially crafted Apple QuickTime file.
CVE-2018-5816	An integer overflow error within the "identify()" function (internal/dcraw_common.cpp) in LibRaw versions prior to 0.18.12 can be exploited to trigger a division by zero via specially crafted NOKIARAW file (Note:

	This vulnerability is caused due to an incomplete fix of CVE-2018-5804).
CVE-2018-5950	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-2018-6003	An issue was discovered in the _asn1_decode_simple_ber function in decoding.c in GNU Libtasn1 before 4.13. Unlimited recursion in the BER decoder leads to stack exhaustion and DoS.
CVE-2018-6031	Use after free in PDFium in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2018-6032	Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user cross-origin data via a crafted HTML page.
CVE-2018-6033	Insufficient data validation in Downloads in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially run arbitrary code outside sandbox via a crafted Chrome Extension.
CVE-2018-6034	Insufficient data validation in WebGL in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6035	Insufficient policy enforcement in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user local file data via a crafted Chrome Extension.
CVE-2018-6036	Insufficient data validation in V8 in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user data via a crafted HTML page.
CVE-2018-6037	Inappropriate implementation in autofill in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to obtain autofill data with insufficient user gestures via a crafted HTML page.
CVE-2018-6038	Heap buffer overflow in WebGL in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6039	Insufficient data validation in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user cross-origin data via a crafted Chrome Extension.
CVE-2018-6040	Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially bypass content security policy via a crafted HTML page.

CVE-2018-6041	Incorrect security UI in navigation in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6042	Incorrect security UI in Omnibox in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6043	Insufficient data validation in External Protocol Handler in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially execute arbitrary programs on user machine via a crafted HTML page.
CVE-2018-6044	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6045	Insufficient policy enforcement in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user local file data via a crafted Chrome Extension.
CVE-2018-6046	Insufficient data validation in DevTools in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user cross-origin data via a crafted Chrome Extension.
CVE-2018-6047	Insufficient policy enforcement in WebGL in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak user redirect URL via a crafted HTML page.
CVE-2018-6048	Insufficient policy enforcement in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially leak referrer information via a crafted HTML page.
CVE-2018-6049	Incorrect security UI in permissions prompt in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the origin to which permission is granted via a crafted HTML page.
CVE-2018-6050	Incorrect security UI in Omnibox in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6051	XSS Auditor in Google Chrome prior to 64.0.3282.119, did not ensure the reporting URL was in the same origin as the page it was on, which allowed a remote attacker to obtain referrer details via a crafted HTML page.
CVE-2018-6052	Lack of support for a non standard no-referrer policy value in Blink in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to obtain referrer details from

	a web page that had thought it had opted out of sending referrer data.
CVE-2018-6053	Inappropriate implementation in New Tab Page in Google Chrome prior to 64.0.3282.119 allowed a local attacker to view website thumbnail images after clearing browser data via a crafted HTML page.
CVE-2018-6054	Use after free in WebUI in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially exploit heap corruption via a crafted Chrome Extension.
CVE-2018-6055	Insufficient policy enforcement in Catalog Service in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to potentially run arbitrary code outside sandbox via a crafted HTML page.
CVE-2018-6056	Type confusion could lead to a heap out-of-bounds write in V8 in Google Chrome prior to 64.0.3282.168 allowing a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-6057	Lack of special casing of Android ashmem in Google Chrome prior to 65.0.3325.146 allowed a remote attacker who had compromised the renderer process to bypass inter-process read only guarantees via a crafted HTML page.
CVE-2018-6058	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6059	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6060	Use after free in WebAudio in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6061	A race in the handling of SharedArrayBuffers in WebAssembly in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6062	Heap overflow write in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6063	Incorrect use of mojo::WrapSharedMemoryHandle in Mojo in Google Chrome prior to 65.0.3325.146 allowed a remote attacker who had compromised the renderer process to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6064	Type Confusion in the implementation of __defineGetter__ in V8 in Google Chrome prior to

	65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6065	Integer overflow in computing the required allocation size when instantiating a new javascript object in V8 in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6066	Lack of CORS checking by ResourceFetcher/ ResourceLoader in Blink in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6067	Incorrect IPC serialization in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6068	Object lifecycle issue in Chrome Custom Tab in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6069	Stack buffer overflow in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6070	Lack of CSP enforcement on WebUI pages in Bink in Google Chrome prior to 65.0.3325.146 allowed an attacker who convinced a user to install a malicious extension to bypass content security policy via a crafted Chrome Extension.
CVE-2018-6071	An integer overflow in Skia in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2018-6072	An integer overflow leading to use after free in PDFium in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file.
CVE-2018-6073	A heap buffer overflow in WebGL in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6074	Failure to apply Mark-of-the-Web in Downloads in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to bypass OS level controls via a crafted HTML page.
CVE-2018-6075	Incorrect handling of specified filenames in file downloads in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page and user interaction.
CVE-2018-6076	Insufficient encoding of URL fragment identifiers in Blink in Google Chrome prior to 65.0.3325.146 allowed a

	remote attacker to perform a DOM based XSS attack via a crafted HTML page.
CVE-2018-6077	Displacement map filters being applied to cross-origin images in Blink SVG rendering in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6078	Incorrect handling of confusable characters in Omnibox in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-6079	Inappropriate sharing of TEXTURE_2D_ARRAY/ TEXTURE_3D data between tabs in WebGL in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6080	Lack of access control checks in Instrumentation in Google Chrome prior to 65.0.3325.146 allowed a remote attacker who had compromised the renderer process to obtain memory metadata from privileged processes .
CVE-2018-6081	XSS vulnerabilities in Interstitials in Google Chrome prior to 65.0.3325.146 allowed an attacker who convinced a user to install a malicious extension or open Developer Console to inject arbitrary scripts or HTML via a crafted HTML page.
CVE-2018-6082	Including port 22 in the list of allowed FTP ports in Networking in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to potentially enumerate internal host services via a crafted HTML page.
CVE-2018-6083	Failure to disallow PWA installation from CSP sandboxed pages in AppManifest in Google Chrome prior to 65.0.3325.146 allowed a remote attacker to access privileged APIs via a crafted HTML page.
CVE-2018-6085	Re-entry of a destructor in Networking Disk Cache in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2018-6086	A double-eviction in the Incognito mode cache that lead to a user-after-free in Networking Disk Cache in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code via a crafted HTML page.
CVE-2018-6087	A use-after-free in WebAssembly in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-6088	An iterator-invalidation bug in PDFium in Google Chrome prior to 66.0.3359.117 allowed a remote

	attacker to execute arbitrary code inside a sandbox via a crafted PDF file.
CVE-2018-6089	A lack of CORS checks, after a Service Worker redirected to a cross-origin PDF, in Service Worker in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak limited cross-origin data via a crafted HTML page.
CVE-2018-6090	An integer overflow that lead to a heap buffer-overflow in Skia in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-6091	Service Workers can intercept any request made by an <embed> or <object> tag in Fetch API in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6092	An integer overflow on 32-bit systems in WebAssembly in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page.
CVE-2018-6093	Insufficient origin checks in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak cross-origin data via a crafted HTML page.
CVE-2018-6094	Inline metadata in GarbageCollection in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2018-6095	Inappropriate dismissal of file picker on keyboard events in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to read local files via a crafted HTML page.
CVE-2018-6096	A JavaScript focused window could overlap the fullscreen notification in Fullscreen in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to obscure the full screen warning via a crafted HTML page.
CVE-2018-6097	Incorrect handling of asynchronous methods in Fullscreen in Google Chrome on macOS prior to 66.0.3359.117 allowed a remote attacker to enter full screen without showing a warning via a crafted HTML page.
CVE-2018-6098	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6099	A lack of CORS checks in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to leak limited cross-origin data via a crafted HTML page.

CVE-2018-6100	Incorrect handling of confusable characters in URL Formatter in Google Chrome on macOS prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6101	A lack of host validation in DevTools in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to execute arbitrary code via a crafted HTML page, if the user is running a remote DevTools debugging server.
CVE-2018-6102	Missing confusable characters in Internationalization in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted domain name.
CVE-2018-6103	A stagnant permission prompt in Prompts in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to bypass permission policy via a crafted HTML page.
CVE-2018-6104	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6105	Incorrect handling of confusable characters in Omnibox in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6106	An asynchronous generator may return an incorrect state in V8 in Google Chrome prior to 66.0.3359.117 allowing a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2018-6107	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted domain name.
CVE-2018-6108	Incorrect handling of confusable characters in URL Formatter in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via IDN homographs via a crafted HTML page.
CVE-2018-6109	readAsText() can indefinitely read the file picked by the user, rather than only once at the time the file is picked in File API in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to access data on the user file system without explicit consent via a crafted HTML page.
CVE-2018-6110	Parsing documents as HTML in Downloads in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to cause Chrome to execute scripts via a local non-HTML page.
CVE-2018-6111	An object lifetime issue in the developer tools network handler in Google Chrome prior to 66.0.3359.117

	allowed a local attacker to execute arbitrary code via a crafted HTML page.
CVE-2018-6112	Making URLs clickable and allowing them to be styled in DevTools in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page.
CVE-2018-6113	Improper handling of pending navigation entries in Navigation in Google Chrome on iOS prior to 66.0.3359.117 allowed a remote attacker to perform domain spoofing via a crafted HTML page.
CVE-2018-6114	Incorrect enforcement of CSP for <object> tags in Blink in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to bypass content security policy via a crafted HTML page.
CVE-2018-6115	Inappropriate setting of the SEE_MASK_FLAG_NO_UI flag in file downloads in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to potentially bypass OS malware checks via a crafted HTML page.
CVE-2018-6116	A nullptr dereference in WebAssembly in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to potentially perform out of bounds memory access via a crafted HTML page.
CVE-2018-6117	Confusing settings in Autofill in Google Chrome prior to 66.0.3359.117 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page.
CVE-2018-6119	Incorrect security UI in Omnibox in Google Chrome prior to 64.0.3282.119 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.
CVE-2018-6120	An integer overflow that could lead to an attacker-controlled heap out-of-bounds write in PDFium in Google Chrome prior to 66.0.3359.170 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted PDF file.
CVE-2018-6121	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6122	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6123	A use after free in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.

CVE-2018-6124	Type confusion in ReadableStreams in Blink in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page.
CVE-2018-6125	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6126	A precision error in Skia in Google Chrome prior to 67.0.3396.62 allowed a remote attacker to perform an out of bounds memory write via a crafted HTML page.
CVE-2018-6127	Early free of object in use in IndexDB in Google Chrome prior to 67.0.3396.62 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page.
CVE-2018-6128	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6129	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6130	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6131	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6132	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6133	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	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the

	candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6135	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	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6137	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	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6139	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	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6143	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	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the

	candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6147	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	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6149	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6150	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6151	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	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6155	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6156	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when

	announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6157	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6158	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	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6161	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6162	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	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the

	candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6169	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	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6172	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	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6177	** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.
CVE-2018-6178	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-2018-6196	w3m through 0.5.3 is prone to an infinite recursion flaw in HTMLlineproc0 because the feed_table_block_tag function in table.c does not prevent a negative indent value.
CVE-2018-6197	w3m through 0.5.3 is prone to a NULL pointer dereference flaw in formUpdateBuffer in form.c.
CVE-2018-6198	w3m through 0.5.3 does not properly handle temporary files when the ~/.w3m directory is unwritable, which allows a local attacker to craft a symlink attack to overwrite arbitrary files.
CVE-2018-6249	NVIDIA GPU Display Driver contains a vulnerability in kernel mode layer handler where a NULL pointer dereference may lead to denial of service or potential escalation of privileges.
CVE-2018-6253	NVIDIA GPU Display Driver contains a vulnerability in the DirectX and OpenGL Usermode drivers where a specially crafted pixel shader can cause infinite recursion leading to denial of service.
CVE-2018-6307	LibVNC before commit ca2a5ac02fbbadd0a21fabba779c1ea69173d10b contains heap use-after-free vulnerability in server code of file transfer extension that can result remote code execution.
CVE-2018-6381	In ZZIPlib 0.13.67, there is a segmentation fault caused by invalid memory access in the zzip_disk_fread function (zzip/mmapped.c) because the size variable is not validated against the amount of file->stored data.
CVE-2018-6405	In the ReadDCMImage function in coders/dcm.c in ImageMagick before 7.0.7-23, each redmap, greenmap, and bluemap variable can be overwritten by a new pointer. The previous pointer is lost, which leads to a memory leak. This allows remote attackers to cause a denial of service.
CVE-2018-6484	In ZZIPlib 0.13.67, there is a memory alignment error and bus error in the __zzip_fetch_disk_trailer function of zzip/zip.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted zip file.
CVE-2018-6540	In ZZIPlib 0.13.67, there is a bus error caused by loading of a misaligned address in the zzip_disk_findfirst function of zzip/mmapped.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted zip file.
CVE-2018-6541	In ZZIPlib 0.13.67, there is a bus error caused by loading of a misaligned address (when handling disk64_trailer local entries) in __zzip_fetch_disk_trailer (zzip/zip.c). Remote attackers could leverage this

	vulnerability to cause a denial of service via a crafted zip file.
CVE-2018-6552	Apport does not properly handle crashes originating from a PID namespace allowing local users to create certain files as root which an attacker could leverage to perform a denial of service via resource exhaustion, possibly gain root privileges, or escape from containers. The is_same_ns() function returns True when /proc/<global pid>/ does not exist in order to indicate that the crash should be handled in the global namespace rather than inside of a container. However, the portion of the data/apport code that decides whether or not to forward a crash to a container does not always replace sys.argv[1] with the value stored in the host_pid variable when /proc/<global pid>/ does not exist which results in the container pid being used in the global namespace. This flaw affects versions 2.20.8-0ubuntu4 through 2.20.9-0ubuntu7, 2.20.7-0ubuntu3.7, 2.20.7-0ubuntu3.8, 2.20.1-0ubuntu2.15 through 2.20.1-0ubuntu2.17, and 2.14.1-0ubuntu3.28.
CVE-2018-6553	The CUPS AppArmor profile incorrectly confined the dnssd backend due to use of hard links. A local attacker could possibly use this issue to escape confinement. This flaw affects versions prior to 2.2.7-1ubuntu2.1 in Ubuntu 18.04 LTS, prior to 2.2.4-7ubuntu3.1 in Ubuntu 17.10, prior to 2.1.3-4ubuntu0.5 in Ubuntu 16.04 LTS, and prior to 1.7.2-0ubuntu1.10 in Ubuntu 14.04 LTS.
CVE-2018-6554	Memory leak in the irda_bind function in net/irda/af_irda.c and later in drivers/staging/irda/net/af_irda.c in the Linux kernel before 4.17 allows local users to cause a denial of service (memory consumption) by repeatedly binding an AF_IRDA socket.
CVE-2018-6555	The irda_setsockopt function in net/irda/af_irda.c and later in drivers/staging/irda/net/af_irda.c in the Linux kernel before 4.17 allows local users to cause a denial of service (ias_object use-after-free and system crash) or possibly have unspecified other impact via an AF_IRDA socket.
CVE-2018-6559	The Linux kernel, as used in Ubuntu 18.04 LTS and Ubuntu 18.10, allows local users to obtain names of files in which they would not normally be able to access via an overlayfs mount inside of a user namespace.
CVE-2018-6594	lib/Crypto/PublicKey/ElGamal.py in PyCrypto through 2.6.1 generates weak ElGamal key parameters, which allows attackers to obtain sensitive information by reading ciphertext data (i.e., it does not have semantic security in face of a ciphertext-only attack). The Decisional Diffie-Hellman (DDH) assumption does not hold for PyCrypto's ElGamal implementation.
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-2018-6767	A stack-based buffer over-read in the ParseRiffHeaderConfig function of cli/riff.c file of WavPack 5.1.0 allows a remote attacker to cause a denial-of-service attack or possibly have unspecified other impact via a maliciously crafted RF64 file.
CVE-2018-6789	An issue was discovered in the base64d function in the SMTP listener in Exim before 4.90.1. By sending a handcrafted message, a buffer overflow may happen. This can be used to execute code remotely.
CVE-2018-6797	An issue was discovered in Perl 5.18 through 5.26. A crafted regular expression can cause a heap-based buffer overflow, with control over the bytes written.
CVE-2018-6798	An issue was discovered in Perl 5.22 through 5.26. Matching a crafted locale dependent regular expression can cause a heap-based buffer over-read and potentially information disclosure.
CVE-2018-6869	In ZZIPlib 0.13.68, there is an uncontrolled memory allocation and a crash in the __zzip_parse_root_directory function of zzip/zip.c. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted zip file.
CVE-2018-6871	LibreOffice before 5.4.5 and 6.x before 6.0.1 allows remote attackers to read arbitrary files via =WEBSERVICE calls in a document, which use the COM.MICROSOFT.WEBSERVICE function.
CVE-2018-6913	Heap-based buffer overflow in the pack function in Perl before 5.26.2 allows context-dependent attackers to execute arbitrary code via a large item count.
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-2018-6927	The futex_requeue function in kernel/futex.c in the Linux kernel before 4.14.15 might allow attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact by triggering a negative wake or requeue value.
CVE-2018-6951	An issue was discovered in GNU patch through 2.7.6. There is a segmentation fault, associated with a NULL pointer dereference, leading to a denial of service in the intuit_diff_type function in pch.c, aka a "mangled rename" issue.
CVE-2018-6954	systemd-tmpfiles in systemd through 237 mishandles symlinks present in non-terminal path components,

	which allows local users to obtain ownership of arbitrary files via vectors involving creation of a directory and a file under that directory, and later replacing that directory with a symlink. This occurs even if the fs.protected_symlinks sysctl is turned on.
CVE-2018-7050	An issue was discovered in lrssi before 1.0.7 and 1.1.x before 1.1.1. A NULL pointer dereference occurs for an "empty" nick.
CVE-2018-7051	An issue was discovered in lrssi before 1.0.7 and 1.1.x before 1.1.1. Certain nick names could result in out-of-bounds access when printing theme strings.
CVE-2018-7052	An issue was discovered in lrssi before 1.0.7 and 1.1.x before 1.1.1. When the number of windows exceeds the available space, a crash due to a NULL pointer dereference would occur.
CVE-2018-7053	An issue was discovered in lrssi before 1.0.7 and 1.1.x before 1.1.1. There is a use-after-free when SASL messages are received in an unexpected order.
CVE-2018-7054	An issue was discovered in lrssi before 1.0.7 and 1.1.x before 1.1.1. There is a use-after-free when a server is disconnected during netsplits. NOTE: this issue exists because of an incomplete fix for CVE-2017-7191.
CVE-2018-7073	A local arbitrary file modification vulnerability was identified in HPE Moonshot Provisioning Manager prior to v1.24.
CVE-2018-7183	Buffer overflow in the decodearr function in ntpq in ntp 4.2.8p6 through 4.2.8p10 allows remote attackers to execute arbitrary code by leveraging an ntpq query and sending a response with a crafted array.
CVE-2018-7185	The protocol engine in ntp 4.2.6 before 4.2.8p11 allows a remote attackers to cause a denial of service (disruption) by continually sending a packet with a zero-origin timestamp and source IP address of the "other side" of an interleaved association causing the victim ntpd to reset its association.
CVE-2018-7225	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-2018-7443	The ReadTIFFImage function in coders/tiff.c in ImageMagick 7.0.7-23 Q16 does not properly validate the amount of image data in a file, which allows remote attackers to cause a denial of service (memory allocation failure in the AcquireMagickMemory function in MagickCore/memory.c).
CVE-2018-7456	A NULL Pointer Dereference occurs in the function TIFFPrintDirectory in tif_print.c in LibTIFF 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-2018-7480	The blkcg_init_queue function in block/blk-cgroup.c in the Linux kernel before 4.11 allows local users to cause a denial of service (double free) or possibly have unspecified other impact by triggering a creation failure.
CVE-2018-7492	A NULL pointer dereference was found in the net/rds/rdma.c __rds_rdma_map() function in the Linux kernel before 4.14.7 allowing local attackers to cause a system panic and a denial-of-service, related to RDS_GET_MR and RDS_GET_MR_FOR_DEST.
CVE-2018-7536	An issue was discovered in Django 2.0 before 2.0.3, 1.11 before 1.11.11, and 1.8 before 1.8.19. The django.utils.html.urlize() function was extremely slow to evaluate certain inputs due to catastrophic backtracking vulnerabilities in two regular expressions (only one regular expression for Django 1.8.x). The urlize() function is used to implement the urlize and urlizetrunc template filters, which were thus vulnerable.
CVE-2018-7537	An issue was discovered in Django 2.0 before 2.0.3, 1.11 before 1.11.11, and 1.8 before 1.8.19. If django.utils.text.Truncator's chars() and words() methods were passed the html=True argument, they were extremely slow to evaluate certain inputs due to a catastrophic backtracking vulnerability in a regular expression. The chars() and words() methods are used to implement the truncatechars_html and truncatewords_html template filters, which were thus vulnerable.
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-2018-7566	The Linux kernel 4.15 has a Buffer Overflow via an SNDRV_SEQ_IOCTL_SET_CLIENT_POOL ioctl write operation to /dev/snd/seq by a local user.
CVE-2018-7584	In PHP through 5.6.33, 7.0.x before 7.0.28, 7.1.x through 7.1.14, and 7.2.x through 7.2.2, there is a stack-based buffer under-read while parsing an HTTP response in the php_stream_url_wrap_http_ex

	function in ext/standard/http_fopen_wrapper.c. This subsequently results in copying a large string.
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-2018-7728	An issue was discovered in Exempi through 2.4.4. XMPFiles/source/FileHandlers/TIFF_Handler.cpp mishandles a case of a zero length, leading to a heap-based buffer over-read in the MD5Update() function in third-party/zuid/interfaces/MD5.cpp.
CVE-2018-7729	An issue was discovered in Exempi through 2.4.4. There is a stack-based buffer over-read in the PostScript_MetaHandler::ParsePSFile() function in XMPFiles/source/FileHandlers/PostScript_Handler.cpp.
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_MetaHandler::CacheFileData() function.
CVE-2018-7731	An issue was discovered in Exempi through 2.4.4. XMPFiles/source/FormatSupport/WEBP_Support.cpp does not check whether a bitstream has a NULL value, leading to a NULL pointer dereference in the WEBP::VP8XChunk class.
CVE-2018-7750	transport.py in the SSH server implementation of Paramiko before 1.17.6, 1.18.x before 1.18.5, 2.0.x before 2.0.8, 2.1.x before 2.1.5, 2.2.x before 2.2.3, 2.3.x before 2.3.2, and 2.4.x before 2.4.1 does not properly check whether authentication is completed before processing other requests, as demonstrated by channel-open. A customized SSH client can simply skip the authentication step.
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-2018-7757	Memory leak in the sas_smp_get_phy_events function in drivers/scsi/libsas/sas_expander.c in the Linux kernel through 4.15.7 allows local users to cause a denial of service (memory consumption) via many read

	accesses to files in the /sys/class/sas_phy directory, as demonstrated by the /sys/class/sas_phy/phy-1:0:12/invalid_dword_count file.
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 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.
CVE-2018-8014	The defaults settings for the CORS filter provided in Apache Tomcat 9.0.0.M1 to 9.0.8, 8.5.0 to 8.5.31, 8.0.0.RC1 to 8.0.52, 7.0.41 to 7.0.88 are insecure and enable 'supportsCredentials' for all origins. It is expected that users of the CORS filter will have configured it appropriately for their environment rather than using it in the default configuration. Therefore, it is expected that most users will not be impacted by this issue.
CVE-2018-8034	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.
CVE-2018-8043	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 allows local users to cause a denial of service (NULL pointer dereference).
CVE-2018-8087	Memory leak in the hwsim_new_radio_nl function in drivers/net/wireless/mac80211_hwsim.c in the Linux kernel through 4.15.9 allows local users to cause a denial of service (memory consumption) by triggering an out-of-array error case.
CVE-2018-8777	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-2018-8781	The udl_fb_mmap function in drivers/gpu/drm/udl/udl_fb.c at the Linux kernel version 3.4 and up to and including 4.15 has an integer-overflow vulnerability allowing local users with access to the udldrmfb driver to obtain full read and write permissions on kernel physical pages, resulting in a code execution in kernel space.
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-2018-8822	Incorrect buffer length handling in the ncp_read_kernel function in fs/ncpfs/ncplib_kernel.c in the Linux kernel through 4.15.11, and in drivers/staging/ncpfs/ncplib_kernel.c in the Linux kernel 4.16-rc through 4.16-rc6, could be exploited by malicious NCPFS servers to crash the kernel or execute code.
CVE-2018-8885	screenresolution-mechanism in screen-resolution-extra 0.17.2 does not properly use the PolicyKit D-Bus API, which allows local users to bypass intended access restrictions by leveraging a race condition via a setuid or pkexec process that is mishandled in a PolicyKitService._check_permission call.
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-2018-8960	The ReadTIFFImage function in coders/tiff.c in ImageMagick 7.0.7-26 Q16 does not properly restrict memory allocation, leading to a heap-based buffer over-read.
CVE-2018-9133	ImageMagick 7.0.7-26 Q16 has excessive iteration in the DecodeLabImage and EncodeLabImage functions (coders/tiff.c), which results in a hang (tens of minutes) with a tiny PoC file. Remote attackers could leverage this vulnerability to cause a denial of service via a crafted tiff file.
CVE-2018-9234	GnuPG 2.2.4 and 2.2.5 does not enforce a configuration in which key certification requires an offline master Certify key, which results in apparently valid certifications that occurred only with access to a signing subkey.
CVE-2018-9363	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-2018-9415	In driver_override_store and driver_override_show of bus.c, there is a possible double free due to improper locking. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-69129004 References: Upstream kernel.
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-2018-9918	libqpdf.a in QPDF through 8.0.2 mishandles certain "expected dictionary key but found non-name object" cases, allowing remote attackers to cause a denial of service (stack exhaustion), related to the QPDFObjectHandle and QPDF_Dictionary classes, because nesting in direct objects is not restricted.

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-2019-2420	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.24 and prior and 8.0.13 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-2019-2422	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Libraries). Supported versions that are affected are Java SE: 7u201, 8u192 and 11.0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/ C:L/I:N/A:N).
CVE-2019-2426	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Networking). Supported

	versions that are affected are Java SE: 7u201, 8u192 and 11.0.1; Java SE Embedded: 8u191. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks of this vulnerability can result in unauthorized read access to a subset of Java SE accessible data. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability can also be exploited by using APIs in the specified Component, e.g., through a web service which supplies data to the APIs. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2019-2434	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). Supported versions that are affected are 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-2019-2449	Vulnerability in the Java SE component of Oracle Java SE (subcomponent: Deployment). The supported version that is affected is Java SE: 8u192. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise Java SE. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a partial denial of service (partial DOS) of Java SE. Note: This vulnerability applies to Java deployments, typically in clients running sandboxed Java Web Start applications or sandboxed Java applets (in Java SE 8), that load and run untrusted code (e.g., code that comes from the internet) and rely on the Java sandbox for security. This vulnerability does not apply to Java deployments, typically in servers, that load and run only trusted code (e.g., code installed by an administrator). CVSS 3.0 Base Score 3.1 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:N/I:N/A:L).
CVE-2019-2455	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Parser). 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-2019-2481	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 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-2019-2482	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: PS). 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-2019-2486	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.24 and prior and 8.0.13 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-2019-2503	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-2019-2507	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 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-2019-2510	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.7.24 and prior and 8.0.13 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-2019-2528	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Partition). Supported versions that are affected are 5.7.24 and prior and 8.0.13 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-2019-2529	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-2019-2531	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). 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 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-2019-2532	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.7.24 and prior and 8.0.13 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-2019-2534	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). 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 access to critical data or complete access to all MySQL Server accessible data as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:L/A:N).
CVE-2019-2537	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). 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 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-2019-3813	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-2019-3823	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-2019-5882	Irssi 1.1.x before 1.1.2 has a use after free when hidden lines are expired from the scroll buffer.
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-2019-6110	In OpenSSH 7.9, due to accepting and displaying arbitrary stderr output from the server, a malicious server (or Man-in-The-Middle attacker) can manipulate the client output, for example to use ANSI control codes to hide additional files being transferred.

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

5.4 Passed rules - Runtime Behavior Analysis-1.0

Rule	Description
Insecure client protocols (general)	This rule detects client use of insecure protocols.
Insecure client protocols (login)	This rule detects client use of insecure protocols to login to remote machines.
Root process with insecure permissions	This rule helps detect root processes that load modules that can be modified by unauthorized users.
Software without DEP	This rule detects the presence of third-party software that is compiled without support for DEP. DEP increases system security by defending against stack-based buffer overflow and other memory corruption attacks.

5.5 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.