Security Advisory
Volume 2015-218-1

Product	Description	Affected Versions	Other Information
Symantec Endpoint Protection Multiple Flaws Let Remote Users Bypass Authenticated and Remote Authenticated Users Read/Write Files, Inject SQL Commands, and Gain Elevated Privileges	Multiple vulnerabilities were reported in Symantec Endpoint Protection. A remote authenticated user can gain elevated privileges. A remote authenticated user can read and write files on the target system. A remote authenticated user can inject SQL commands. A remote user can bypass authentication. A remote user can exploit a flaw in the Symantec Endpoint Protection Manager (SEPM) management console's password reset function to bypass authentication and obtain an administrative session [CVE-2015-1486]. A remote authenticated user can exploit a filename validation flaw to write arbitrary files on the target system [CVE-2015-1487]. A remote authenticated user can exploit an action handler validation flaw to read arbitrary files on the target system [CVE-2015-1488]. A remote authenticated user can gain full privileges on the target system [CVE-2015-1489]. A remote authenticated user can create a specifically crafted install package containing an arbitrary relative path to access files on the target system that are located outside of the install folder [CVE-2015-1490]. The software does not properly validate user-supplied input. A remote authenticated user can supply a specially crafted parameter value to execute arbitrary SQL commands on the underlying database [CVE-2015-1491]. A local user on a SEP client can create a specially crafted DLL file and include in in a client install package to cause arbitrary code to be executed on the target system [CVE-2015-1492].	Version(s): 12.1.x prior to 12.1-RU6-MP1	Published - July 31 2015 CVE-2015-1486, CVE-2015-1487, CVE-2015-1488, CVE-2015-1489, CVE-2015-1490, CVE-2015-1491, CVE-2015-1492 CVSS - 8.5 Vendor's Advisory Available at : http://www.symantec.com/security_response/securityupdates/detail.jsp?fid=security_advisory&pvid=security_advisory&year=&suid=20150730_00
Google Android Buffer Overflows in DHCP Let Remote Users Execute Arbitrary Code	Two vulnerabilities were reported in Google Android DHCP. A remote user can execute arbitrary code on the target system. A remote user (server) can return specially crafted DHCP data to trigger a buffer overflow and execute arbitrary code on the target system.	Version(s):	Published - July 22 2015 CVE-2014-7912, CVE-2014-7913 CVSS - 6.4 The vendor's advisory is available at: https://android.googlesource.com/platform/external/dhcpcd/+/73c09dd8067250734511d955d8f792b41c7213f0
Cisco AnyConnect Secure Mobility Client Lets Local Users Cause Denial of Service Conditions on the Target System	A vulnerability was reported in Cisco AnyConnect Secure Mobility Client. A local user can cause denial of service conditions on the target system. A local user can trigger a flaw in the kernel extension for Mac OS X to cause a kernel panic	Version(s):4.0(2049	Published - July 29 2015 CVE-2015-4290 CVSS - 4.9 Vendor's Advisory Available at http://tools.cisco.com/security/center/viewAlert.x?alertId=40176
Linux Kernel Infinite Loop in Processing iso9660 Images Lets Users Deny Service	A vulnerability was reported in the Linux Kernel. A remote or local user can cause denial of service conditions. A remote user can create a specially crafted iso9660 image that, when loaded by the target local user, will cause the init_rock_state() function in 'fs/isofs/rock.c' to enter an infinite loop. The system may crash or become unstable	Version(s): RHEL 6	Published - July 14 2015 CVE-2014-9420 CVSS - 4.9 The vendor's advisory is available at: https://rhn.redhat.com/errata/RHSA-2015-1081.html
Apple iOS Flaws Let Remote Users Deny Service and Execute Arbitrary Code	Multiple vulnerabilities were reported in Apple iOS. A remote user can cause arbitrary code to be executed on the target user's system. A remote user can cause denial of service conditions on the target system. A remote user (universal provisioning profile app) can use the bundle ID of an existing app to prevent the existing app from launching [CVE-2015-3722]. Apple Watch apps are also affected [CVE-2015-3725].A remote user that can conduct a man-in-the-middle attack can use a certificate signed by an incorrectly issued CNNIC certificate authority to bypass trusted certificate validation. A remote user can create a specially crafted PDF file that, when loaded by the target user, will trigger a memory corruption error and execute arbitrary code on the target system. A user can create a specially crafted SIM card that, when physically installed by the target user, will execute arbitrary code	Version(s):prior to 8.4	Published - July 1 2015 CVE-2015-3722, CVE-2015-3723, CVE-2015-3724, CVE-2015-3725, CVE-2015-3726, CVE-2015-3728 CVSS - 4.3 Vendor's Advisory Available at https://support.apple.com/kb/HT204941
OpenSSH 'KbdInteractiveDevices' Lets Remote Users Bypass Security Restrictions on the Target System	A vulnerability was reported in OpenSSH. A remote user can bypass authentication attempt limits on the target system. A remote user can request the keyboard-interactive authentication option ('KbdInteractiveDevices') to open a large number of keyboard-interactive devices on the target server and perform a brute-force password guessing attack against the target sshd service. The number of password attempts can effectively exceed the 'MaxAuthTries' limit and are permitted to occur until the 'LoginGraceTime' limit is reached or the number of keyboard-interactive devices are used. Servers that have keyboard-interactive authentication enabled (e.g., FreeBSD in the default configuration) are affected. A demonstration exploit command is provided: ssh -l[username] -oKbdInteractiveDevices=`perl -e 'print "pam," x 10000'` [target]	Version(s):	Published - July 29 2015 CVE-2015-5600 CVSS - 8.5 The vendor's advisory is available at: https://kingcope.wordpress.com/2015/07/16/openssh-keyboard-interactive-authentication-brute-force-vulnerability-maxauthtries-bypass/
Cisco ASR 1000 Series Routers Fragmented Packet Processing Flaw Lets Remote Users Cause the Target System to Crash	A vulnerability was reported in Cisco ASR 1000 series routers. A remote user can cause the target device to reload. A remote user can send a specially crafted sequence of IPv4 or IPv6 packets to the target IOS-XE ASR 1000 series device to cause the target Embedded Services Processor (ESP) to crash. As a result, the target device will reload.	Version(s):2.1.x - 2.5.x	Published - Jul 30, 2015 CVE-2015-4291 CVSS - 5.0 Vendor's Advisory Available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20150730-asr1k
(Ubuntu) PCRE Regex Overflow Lets Remote Users Cause the Target Service to Crash	Multiple vulnerabilities were reported in Microsoft Internet Explorer. A remote user can cause arbitrary code to be executed on the target user's system. A remote user can gain elevated privileges. A remote user can bypass security controls on the target system. A remote user can obtain potentially sensitive information on the target system. A remote user can conduct cross-site scripting attacks. A vulnerability was reported in PCRE. A remote user can cause the target service to crash. A remote user can supply a specially crafted regular expression that, when processed by the target application that uses PCRE, will trigger a heap overflow in find_fixedlength() and cause the target application to crashRandomization (ASLR) protection features on the target user's system [CVE-2015-2421]. A remote user can create specially crafted content that, when loaded by the target user, will access potentially sensitive information on the target user's system.	Version(s):8.37; possibly other versions	Published - July 31 2015 CVE-2015-5073 CVSS - 6.5 The Source Code Fix is available at: http://www.ubuntu.com/usn/usn-2694-1
Oracle Issues Fix for Oracle Linux) FreeRADIUS SHAA Stack Overflow Lets Remote Users Deny Service in Certain Cases	A vulnerability was reported in FreeRADIUS. A remote user can cause denial of service conditions in certain cases. A remote user with an existing user account and that can specify a specially crafted hashed SHAA password value can trigger a stack overflow in the rlm_pap module and cause the target service to crash.	Version(s):	Published - Jul 14 2015 CVE-2014-2015 CVSS - 5.3 Vendor's Advisory Available at http://linux.oracle.com/errata/ELSA-2015-1287.html

Product	Description	Affected Versions	Other Information
MySQL Multiple Bugs Let Remote and Local Users Deny Service and Remote Authenticated Users Partially Access and Modify Data	Multiple vulnerabilities were reported in MySQL. A remote authenticated user can partially access data on the target system. A remote authenticated user can partially modify data on the target system. A remote or local user can cause partial denial of service conditions on the target system. A remote authenticated user can exploit a flaw in the MySQL Server Partition component to partially access data, partially modify data, and partially deny service [CVE-2015-2617]. A remote authenticated user can exploit a flaw in the MySQL Server DML component to cause partial denial of service conditions [CVE-2015-2648]. A remote authenticated user can exploit a flaw in the MySQL Server DML component to cause partial denial of service conditions [CVE-2015-2611]. A remote authenticated user can exploit a flaw in the MySQL Server GIS component to cause partial denial of service conditions [CVE-2015-2582]. A remote authenticated user can exploit a flaw in the MySQL Server I_S component to cause partial denial of service conditions [CVE-2015-4752]. A remote authenticated user can exploit a flaw in the MySQL Server InnoDB component to cause partial denial of service conditions [CVE-2015-4756]. A remote authenticated user can exploit a flaw in the MySQL Server Optimizer component to cause partial denial of service conditions [CVE-2015-2643]. A remote authenticated user can exploit a flaw in the MySQL Server Partition component to cause partial denial of service conditions [CVE-2015-4772].	Version(s):	Published - Jul 15 2015 CVE-2015-2582, CVE-2015-2611, CVE-2015-2617, CVE-2015-2620, CVE-2015-2639, CVE-2015-2641, CVE-2015-2643, CVE-2015-2648, CVE-2015-2661, CVE-2015-4737, CVE-2015-4752, CVE-2015-4756, CVE-2015-4757, CVE-2015-4761, CVE-2015-4767, CVE-2015-4769, CVE-2015-4771, CVE-2015-4772 CVSS - 5.0 Vendor's Advisory Available at: http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
Oracle Database Multiple Flaws Let Remote Users Access and Modify Data and Deny Service, Remote Authenticated Users Gain Elevated Privileges, and Local Users Access Data	Two vulnerabilities were reported in Microsoft Hyper-V. A local user on the guest system can gain elevated privileges on the host system. A local privileged user on the guest system can run a specially crafted application to trigger a buffer overflow and execute arbitrary code on the host system [CVE-2015-2361]. A local privileged user on the guest system can run a specially crafted application to trigger a data structure error and gain elevated privileges on the host system [CVE-2015-2362].	Version:	Published - Jul 14 2015 CVE-2015-2361, CVE-2015-2362 CVSS - 7.5 Vendor's Advisory Available at https://technet.microsoft.com/library/security/ms15-068
Oracle Database Multiple Flaws Let Remote Users Access and Modify Data and Deny Service, Remote Authenticated Users Gain Elevated Privileges, and Local Users Access Data	Multiple vulnerabilities were reported in Cisco IOS-XE on Cisco ASR 1000, 4400, and 1000v Series Routers. A remote user can execute arbitrary code on the target system. A remote user can cause denial of service conditions on the target system. Multiple vulnerabilities were reported in Oracle Database. A remote or remote authenticated user can access data or modify data on the target system. A remote or remote authenticated user can cause denial of service conditions on the target system. A local user can access data on the target system. A remote authenticated user can gain elevated privileges. A remote authenticated user can exploit a flaw in the Java VM component to gain elevated privileges [CVE-2015-2629]. A remote authenticated user can exploit a flaw in the Oracle OLAP component to partially access data, partially modify data, and partially deny service [CVE-2015-2595]. A remote authenticated user can exploit a flaw in the Core RDBMS component to partially access data, partially modify data, and partially deny service [CVE-2015-0468]. A remote authenticated user can exploit a flaw in the RDBMS Partitioning component to partially access data, partially modify data, and partially deny service [CVE-2015-4740]. A remote authenticated user can exploit a flaw in the Application Express component to partially access and partially modify data [CVE-2015-2655]. A remote user can exploit a flaw in the RDBMS Security component to partially access data [CVE-2015-4755]. A remote user can exploit a flaw in the Application Express component to cause partial denial of service conditions [CVE-2015-2586]. A remote authenticated user can exploit a flaw in the RDBMS Scheduler component to partially access data [CVE-2015-	Version:11.1.0.7, 11.2.0.3, 11.2.0.4, 12.1.0.1, 12.1.0.2	Published - Jul 14 2015 CVE-2015-0468, CVE-2015-2585, CVE-2015-2586, CVE-2015-2595, CVE-2015-2599, CVE-2015-2629, CVE-2015-2655, CVE-2015-4740, CVE-2015-4753, CVE-2015-4755 CVSS - 7.8 Vendor's Advisory Available at http://www.oracle.com/technetwork/topics/security/cpujul2015-2367936.html
Microsoft SQL Server Bugs Let Remote Authenticated Users Gain Privilege Escalation and Execute Arbitrary Code	Several vulnerabilities were reported in Microsoft SQL Server. A remote authenticated user can gain elevated privileges. A remote authenticated user can execute arbitrary code on the target system. A remote authenticated user can send specially crafted SQL data to trigger a pointer casting error and gain elevated privileges on the target database [CVE-2015-1761]. This can be exploited to view, change, or delete data and to create new accounts. A remote authenticated privileged user can send a specially crafted SQL query to trigger a function call initialization error and execute arbitrary code on the target system [CVE-2015-1762]. This can be exploited to install programs, view, change, or delete data, or create new accounts. Servers that have special permission settings (e.g., VIEW SERVER STATE) enabled are affected. A remote authenticated user can send a specially crafted SQL query to trigger a function call initialization error and execute arbitrary code on the target system [CVE-2015-1763]. This can be exploited to install programs, view, change, or delete data, or create new accounts.	Version:2008 SP3, 2008 SP4, 2008 R2 SP2, 2008 R2 SP3, 2012 SP1, 2012 SP2, 2014	Published - July 14 2015 CVE-2015-1761, CVE-2015-1762, CVE-2015-1763 CVSS - 7.1 Vendor's Advisory Available : https://technet.microsoft.com/library/security/ms15-058