Product	Description	Affected Versions	Other Information
OpenSSH TTY Permissions Let Local Users Cause Denial of Service Conditions	A vulnerability was reported in OpenSSH. A local user can cause denial of service conditions on the target system. The system sets TTYs with world-writable permissions. A local user may be able to write arbitrary messages, including escape sequences, to other users on the target system.	Version(s):6.8, 6.9	Published - Oct 22 2015 CVE-2015-6565 CVSS - 7.2 Vendor's Advisory Available at : http://www.openssh.com/txt/release-7.0
Cisco ASA Input Validation Flaw in DHCPv6 Relay Feature Lets Remote Users Cause the Target System to Crash	A vulnerability was reported in Cisco ASA. A remote user can cause the target system to crash. A remote user can send specially crafted DHCPv6 packets to an interface on the target device that is configured with the DHCPv6 relay feature to cause the target device to reload.	Version(s):9.2(1)	Published - Oct 21 2015 CVE-2015-6324 CVSS - 7.1 http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-dhcp1
Cisco ASA DNS Response Packet Processing Bug Lets Remote Users Cause the Target System to Reload	A vulnerability was reported in Cisco ASA. A remote user can cause the target system to reload. A remote user can return a specially crafted DNS response packet to the target device to cause the target device to reload. Systems configured in routed or transparent firewall mode and single or multiple context mode are affected. Systems with at least one DNS server IP address configured under a DNS server group are affected	Version(s):9.2(1)	Published - Oct 21 2015 CVE-2015-6325 CVSS - 7.2 Vendor's Advisory Available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-dns1
Cisco ASA ISAKMP Processing Flaw Lets Remote Users Cause the Target System to Reload	A vulnerability was reported in Cisco ASA. A remote user can cause the target system to reload. A remote user can send specially crafted ISAKMP UDP packets to the target system to trigger a flaw in the Internet Key Exchange (IKE) version 1 code and cause the target system to reload. Systems configured in routed firewall mode only and in single or multiple context mode are affected.	Version(s):9.2(1)	Published - Oct 21 2015 CVE-2015-6327 CVSS - 7.8 The vendor's advisory is available at: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151021-asa-ike
phpMyAdmin Bug in Redirection Mechanism Lets Remote Users Spoof Content	A vulnerability was reported in phpMyAdmin. A remote user can spoof content. A remote user can invoke the redirection mechanism to spoof content when redirecting the target user to an external site.	Version(s) :4.4.0 to prior to 4.4.15.1, 4.5.0.x	Published - Oct 29 2015 CVE-2015-7873 CVSS - 5.0 Vendor's Advisory Available at https://www.phpmyadmin.net/security/PMASA-2015-5/
Google Android Multiple Flaws Let Remote Users Execute Arbitrary Code and Applications Gain Elevated Privileges	Multiple vulnerabilities were reported in Google Android. A remote user can cause arbitrary code to be executed on the target user's system. An application can gain elevated privileges. A remote user can create a specially crafted file that, when loaded by the target user, will trigger a memory corruption error in Mediaserver and execute arbitrary code on the target system [CVE-2015-6608]. The code will run with the privileges of the mediaserver service, which has access to audio and video streams A remote user can create a specially crafted audio file that, when loaded by the target user, will trigger a memory corruption error in libutils and execute arbitrary code on the target system [CVE-2015-6609]. A user can exploit unspecified flaws in Mediaserver to bypass security measures and obtain potentially sensitive information [CVE-2015-6611]. An application can trigger a memory corruption error in libstagefright to execute arbitrary code and gain elevated privileges on the target system [CVE-2015-6610]. An application can trigger a memory corruption error in libmedia to execute arbitrary code and gain elevated privileges on the target system [CVE-2015-6612]. An application can send commands to a listening debug port on the target system to potentially gain elevated privileges, such as Signature or SignatureOrSystem privileges on the target system [CVE-2015-6613]. An application can pass data to the restricted network interfaces, resulting in telecommunications data charges or preventing incoming calls or controlling the mute settings on calls [CVE-2015-6614].	Version(s) :	Published - Nov 4 2015 CVE-2015-6608, CVE-2015-6609, CVE-2015-6610, CVE-2015-6611, CVE-2015-6612, CVE-2015-6613, CVE-2015-6614 CVSS - 5.0 The vendor's advisory is available at: https://groups.google.com/forum/#!topic/android-security-updates/n1aw2MGce4E
Oracle Supply Chain Products Suite Bugs Let Remote Users Access and Modify Data	Multiple vulnerabilities were reported in Oracle Supply Chain Products Suite. A remote user can access and modify data on the target system. A remote user can exploit a flaw in the Oracle Configurator Integration with PeopleSoft component to partially access data [CVE-2015-4848]. A remote user can exploit a flaw in the Oracle Configurator OCI component to partially modify data [CVE-2015-4847]. A remote authenticated user can exploit a flaw in the Oracle Agile PLM Security component to partially modify data [CVE-2015-4797, CVE-2015-4824, CVE-2015-4892, CVE-2015-4917].	Version(s):	Published - Oct 21 2015 CVE-2015-4797, CVE-2015-4824, CVE-2015-4847, CVE-2015-4848, CVE-2015-4892, CVE-2015-4917 CVSS - 6.0 Vendor's Advisory Available at http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html
Mozilla Firefox Multiple Flaws Let Remote Users Execute Arbitrary Code, Obtain Potentially Sensitive Information, Bypass Security Restrictions, and Conduct Cross-Site Scripting Attacks	Multiple vulnerabilities were reported in Mozilla Firefox. A remote user can cause arbitrary code to be executed on the target user's system. 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 remote user can create specially crafted content that, when loaded by the target user, will trigger a memory corruption error and execute arbitrary code on the target user's system [CVE-2015-4513, CVE-2015-4514]. A remote user can submit an NTLM request (via HTTP) to determine the hostname and potentially the Windows domain of the target system [CVE-2015-4515] The Reader View does not properly disable script code in SVG animations in certain cases [CVE-2015-4518]. A remote user can bypass Reader mode security protections to potentially cause arbitrary scripting code to be executed by the target user's browser. The code will originate from an arbitrary site and will run in the security context of that site. As a result, the code will be able to access the target user's cookies (including authentication cookies), if any, associated with the site, access data recently submitted by the target user via web form to the site, or take actions on the site acting as the target user. On Firefox for Android, the system may not restore the address bar when exiting fullscreen mode. A remote user may be able to exploit this to spoof the address bar [CVE-2015-7185]. On Firefox for Android, an application may be able to invoke "file://" URIs to download additional files or open cached profile data [CVE-2015-7186]. When a panel is created using the Add-on SDK in a browser extension with the "script: false" setting, the system may not disable the execution of inline script [CVE-2015-7187]. A user can append white-space characters to hostnames that are IP addresses to bypass same-origin policy and potentially conduct cross-site scripting attacks [CVE-2015-7188]. A remote user can trigger a buffer overflow in the JPEGEncoder function during script interactions with a canvas element and potentially execute arbitrary code [CVE-2015-7189]. On Firefox for Android, a remote user may be able to exploit a flaw in the Search feature to load a URL with system privileges and read arbitrary files on the target system [CVE-2015-7190].	Version(s):prior to 42.0	Published -Nov 5 2015 CVE-2015-4513, CVE-2015-4514, CVE-2015-4515, CVE-2015-4518, CVE-2015-7181, CVE-2015-7182, CVE-2015-7183, CVE-2015-7185, CVE-2015-7186, CVE-2015-7187, CVE-2015-7188, CVE-2015-7189, CVE-2015-7190, CVE-2015-7191, CVE-2015-7192, CVE-2015-7193, CVE-2015-7194, CVE-2015-7195, CVE-2015-7196, CVE-2015-7197, CVE-2015-7198, CVE-2015-7199, CVE-2015-7200 CVSS - 7.2 Vendor's Advisory Available at: https://www.mozilla.org/en-US/security/advisories/mfsa2015-116/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-117/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-118/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-119/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-120/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-121/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-122/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-123/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-124/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-125/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-126/ https://www.mozilla.org/en-US/security/advisories/mfsa2015-127/
HP ArcSight SmartConnectors Default Password and Lack of Certificate Validation Let Remote Users Gain Access to the Target System or Modify Log Data	Two vulnerabilities were reported in HP ArcSight SmartConnectors. A remote user can access and modify log data. A remote user can gain access to the target system. The system does not properly validate the SSL certificate of the upstream Logger device [CVE-2015-2902]. A remote user with the ability to conduct a man-in-the-middle attack can obtain or modify log data. The system uses a default password that cannot be changed for the CWSAPI SOAP service. A remote user can use the password to access the system with administrator privileges.	Version(s):prior to 7.1.6	Published - Nov 5 2015 CVE-2015-2902, CVE-2015-2903 CVSS - 6.9 Vendor's Advisory Available at https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04850932
HP ArcSight Enterprise Security Manager Unsafe File Permissions Let Local Users Gain Elevated Privileges	A vulnerability was reported in HP ArcSight Enterprise Security Manager. A local user can obtain elevated privileges on the target system. Some files executed by root-owned processes are owned by the "ArcSight" user. A local user can execute arbitrary commands on the target system with root privileges.	Version(s):6.x prior to 6.5SP1P2	Published - Nov 5 2015 CVE-2015-6030 CVSS - 7.2 Vendor's Advisory Available https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04872416
HP ArcSight SmartConnectors Unsafe File Permissions Let Local Users Gain Elevated Privileges	A vulnerability was reported in HP ArcSight SmartConnectors. A local user can obtain elevated privileges on the target system. Some files executed by root-owned processes are owned by the "ArcSight" user. A local user can execute arbitrary commands on the target system with root privileges. HP ArcSight SmartConnectors are not vulnerable if installed as a non-root user.	Version:prior to 7.1.4	Published -Nov 5 2015 CVE-2015-6030 CVSS - 7.2 Vendor's Advisory Available at https://h20564.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c04872416