Security Advisory
Volume 2015-341-1

Product	Description	Affected Versions	Other Information
Apple Remote Desktop Full Screen Sleep Mode Flaw Lets Local Users Bypass Security Restrictions	A vulnerability was reported in Apple Remote Desktop. A local user can bypass security restrictions. A physically local user can bypass security controls on the target system when Apple Remote Desktop is in full screen mode with an active remote connection and the system recovers from sleep mode due to a flaw in dialog box text processing.	Version(s):prior 10.8	Published - Nov 20 2015 CVE-2013-5229 CVSS - 3.7 Vendor's Advisory Available at : www.apple.com/
Red Hat Enterprise Linux Grub2 Bug Lets Local Users Bypass Secure Boot	A vulnerability was reported in Red Hat Enterprise Linux grub2. A local user can bypass secure boot. A local user can invoke the multiboot and multiboot2 modules to execute arbitrary code and bypass Secure Boot restrictions.	Version(s):RHEL 7	Published - Nov 20 2015 CVE-2015-5281 CVSS - 2.6 Vendor's Advisory Available at: rhn.redhat.com/errata/RHSA-2015-2401.html
Adobe LiveCycle XML Document Processing Flaw Lets Remote Users Conduct Cross-Site Request Forgery Attack	A vulnerability was reported in Adobe LiveCycle. A remote user can conduct cross-site request forgery attacks. A remote user can create a specially crafted XML document that, when loaded by the target authenticated user, will take actions on the target interface acting as the target user. The vulnerability resides in the BlazeDS component.	Version(s):3.0.x, 3.1.x, 4.5, 4.6.2, 4.7	Published - Nov 20 2015 CVE-2015-5255 CVSS - 4.3 Vendor's Advisory Available at https://helpx.adobe.com/security/products/livecycleds/apsb15-30.html
Adobe ColdFusion Input Validation Flaws Lets Remote Conduct Cross-Site Scripting Attacks	Two vulnerabilities were reported in Adobe ColdFusion. A remote user can conduct cross-site scripting attacks. The software does not properly filter HTML code from user-supplied input before displaying the input. A remote user can cause arbitrary scripting code to be executed by the target user's browser. The code will originate from the site running the Adobe ColdFusion software 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.	Version(s):10 Update 17 and prior, 11 Update 6 and prior	Published - Nov 20 2015 CVE-2015-8052, CVE-2015-8053 CVSS - 4.3 The vendor's advisory is available at: https://helpx.adobe.com/security/products/coldfusion/apsb15-29.html
Cisco ASA Management Interface XML Parsing Flaw Lets Remote Authenticated Users Cause the Target System to Become Unstable or Crash	A vulnerability was reported in Cisco ASA. A remote authenticated user can cause the target system to become unstable or potentially crash. A remote authenticated user on the management interface can cause the target component to read a specially crafted XML file to trigger a flaw in the XML parser. As a result, the target system will become unstable and may crash. The vendor has assigned bug ID CSCut14223 to this vulnerability.	Version(s) :8.4	Published -Nov 25 2015 CVE-2015-6379 CVSS - 6.8 Vendor's Advisory Available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151123-asa
Cisco ASR 5000 Series Router Telnet Bug Lets Remote Users Cause the Target Service to Crash	A vulnerability was reported in Cisco ASR Router. A remote user can cause the target service to crash. A remote user can exploit a flaw in the Telnet implementation to cause the target telnetd process to restart.	Version(s) :ASR 5000 Series; 16.0(900)	Published - Nov 26 2015 CVE-2015-6382 CVSS - 5.0 The vendor's advisory is available at: http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151125-asr5000
Cisco Cloud Services Router Command Injection Flaw Lets Local Users Obtain Root Privileges	A vulnerability was reported in Cisco IOS on Cisco Cloud Services Router 1000V Series devices. A local user can obtain root privileges on the target system. A local administrative user can exploit a command injection flaw in the event manager environment and publish-event function to execute arbitrary commands on the target system with root privileges. The user can modify the configuration of the device and then invoke a specially crafted event manager script to trigger the vulnerability.	Version(s): Cisco Cloud Services Router 1000V Series; 15.5(2)S and 15.5(3)S	Published - Dec 2 2015 CVE-2015-6061 CVSS - 5.0 Vendor's Advisory Available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151130-csr
Cisco Web Security Appliance FTP Pass-through Lets Remote Users Consume Excessive CPU Resources on the Target System	A vulnerability was reported in Cisco Web Security Appliance. A remote user can consume excessive CPU resources on the target system. A remote user can initiate and then terminate FTP connections through the target system in a specific manner to exploit a flaw in the native pass-through FTP processing function and consume excessive CPU resources on the target system. The vendor has assigned bug ID CSCut94150 to this vulnerability.	Version(s):8.0.7-142, 8.5.1-021	Published - Dec 2 2015 CVE-2015-6386 CVSS - 5.0 Vendor's Advisory Available at http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20151130-wsa
OpenSSH PAM Privilege Separation Bugs Lets Remote Users Gain Elevated Privileges in Certain Cases	Two vulnerabilities were reported in OpenSSH. A remote user can gain elevated privileges in certain cases. A remote user that can exploit a separate vulnerability in the unprivileged pre-authentication process to execute arbitrary code can then exploit two separate flaws in sshd(8) to bypass privilege separation controls [CVE-2015-6563, CVE-2015-6564].	Version(s):6.9p1 and prior	Published - Nov 20 2015 CVE-2015-6563, CVE-2015-6564 CVSS - 5.0 Vendor's Advisory Available at https://rhn.redhat.com/errata/RHSA-2015-2088.html
OpenSSH Bug Lets Remote Authenticated Users Bypass XSECURITY Timeout Security Restrictions	A vulnerability was reported in OpenSSH. A remote authenticated user can bypass security restrictions. A remote authenticated user with a forwarded X11 connection can bypass XSECURITY restrictions to continue the connection after the ForwardX11Timeout has expired.	Version(s):prior to 6.9	Published - Nov 24 2015 CVE-2015-5352 CVSS - 4.3 Vendor's Advisory Available http://linux.oracle.com/errata/ELSA-2015-2088.html
Glibc Buffer Overflow in vfscanf May Let Remote or Local Users Execute Arbitrary Code	Several vulnerabilities were reported in Glibc. A remote or local user may be able to execute arbitrary code on the target system. A remote or local user can cause denial of service conditions on the target system. A remote user can send specially crafted data to an application that uses glibc to trigger a buffer overflow and potentially execute arbitrary code on the target system [CVE-2015-1472]. The code will run with the privileges of the target application. The vulnerability resides in 'stdio-common/vfscanf.c'. A remote or local user can send specially crafted data to an application that uses glibc to cause __libc_use_alloca() to enforce a different memory allocation policy and potentially deny service on the target application [CVE-2015-1473].	Version:prior to 2.21	Published -Nov 28 2015 CVE-2015-1472, CVE-2015-1473 CVSS - 7.8 Vendor's Advisory Available at http://linux.oracle.com/errata/ELSA-2015-2199.html