Security Advisory | Volume 2016-283-1

PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Cisco NX-OS on Nexus 7000 and 7700 Remote Code Execution or DoS in Overlay Transport Virtualization GRE Feature	Buffer overflow in the Overlay Transport Virtualization (OTV) GRE feature in Cisco NX-OS 5.0(3) through 7.3 on Nexus 7000 and Cisco NX-OS 6.2(2) through 7.3 on Nexus 7700 devices allows remote attackers to execute arbitrary code via long parameters in a packet header or reload an affected device, aka Bug ID CSCuy95701.	Version(s): Nexus 7000 Series Switches Nexus 7700 Series Switches	Published - October 05,2016 CVE-2016-1453 CVSS - 10.0 Vendor's Advisory Available at :https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20161005-otv
Remote Code Execution due to a Use-After-Free Vulnerability in Linux Kernel	Linux Kernel networking subsystem, as used in Google Android 7.0 and earlier before 2016-10-05, on all Nexus devices, allows remote attackers to execute arbitrary code in the context of the kernel due to a use-after-free vulnerability in the __sys_recvmmsg function in socket.c, aka Android internal bug 30515201.	Version(s):before 3.19.x, , Google Pixel C 0,Google Nexus Player 0 Google Nexus 9 ,7 (2013), 6P, 6, 5X, 5, Google Android One 0	Published - October 03,2016 CVE-2016-7117 CVSS - 9.3 Vendor's Advisory Available at: https://source.android.com/security/bulletin/2016-10-01.html
Adobe Flash Player Remote Code Execution due to Use-After-Free Vulnerability	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.	Version(s) : 1Adobe Flash Player Desktop Runtime 22.0.0.192 and earlier, Adobe Flash Player Extended Support Release 18.0.0.360 and earlier ,Adobe Flash Player for Google Chrome 22.0.0.192 and earlier ,Adobe Flash Player for Microsoft Edge and Internet Explorer 11 22.0.0.192 and earlier Adobe Flash Player for Linux 11.2.202.626 and earlier	Published - October 03,2016 CVE-2016-7020 CVSS - 9.3 Vendor's Advisory Available at: https://helpx.adobe.com/security/products/flash-player/apsb16-25.html
OpenSSL 1.1.0a Remote DoS or Code Execution via Crafted TLS Session	statem/statem.c in OpenSSL 1.1.0a does not consider memory-block movement after a realloc call, which allows remote attackers to cause a denial of service (use-after-free) or possibly execute arbitrary code via a crafted TLS session.	Version(s) : OpenSSL Project OpenSSL 1.1 , 1.1.0a	Published - September 26,2016 CVE-2016-6309 CVSS - 10.0 The vendor's advisory is available at: http://www.securityfocus.com/bid/93177
Adobe Digital Editions <4.5.2 Remote Code Execution via Unspecified Vectors	Use-after-free vulnerability in Adobe Digital Editions before 4.5.2 allows attackers to execute arbitrary code via unspecified vectors, a different vulnerability than CVE-2016-4263.	Version(s) : Adobe Digital Editions 4.5.1 and earlier versions	Published -September 26,2016 CVE-2016-6980 CVSS - 9.3 Vendor's Advisory Available at https://helpx.adobe.com/security/products/Digital-Editions/apsb16-28.html
Google Chrome OS <53.0.2785.144 Unspecified Vulnerability due to Heap Overflow in C-Ares	Google Chrome OS before 53.0.2785.144 is prone to unspecified vulnerability due to heap overflow in c-ares.	Version(s) : Google Chrome OS before 53.0.2785.144	Published -September 30,2016 CVE-2016-5180 CVSS - 9.3 The vendor's advisory is available at: http://www.securityfocus.com/bid/93243
Google Android <=7.0 on Nexus Devices Unspecified Vulnerability via Unspecified Vectors	Google Android 7.0 and earlier before 2016-10-05 on Nexus 5X and 6P devices are prone to an unspecified vulnerability via unspecified vectors with unspecified impact, aka Android Bug ID: A-28823675	Version(s)Google Nexus 6P Google Nexus 6 Google Nexus 5X Google Nexus 5 Google Android 0	Published - October 05,2016 CVE-2016-3929, CVE-2016-3927,CVE-2016-3926 CVSS -10.0 Vendor's Advisory Available at https://source.android.com/security/bulletin/2016-10-01.html
Google Android 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0 Remote Elevation of Privileges in Telephony Component	Google Android versions 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1 and 7.0 before 1st October 2016 are prone to an elevation of privileges vulnerability in the Telephony component. The flaw could enable a crafted application to execute arbitrary code in the context of a privileged process. AKA Android internal bug A-30481342.	Version(s) : Google Pixel C 0 Google Nexus Player 0 Google Nexus 9, 7 (2013) Google Nexus 6P, 6, 5X, 5 Google Android One 0, 6.0.1 , 5.1.1 , 5.0.2 ,Google Android 4.4.4 ,d 7.0, 6.0	Published - October 01, 2016 CVE-2016-3914 CVSS - 9.3 Vendor's Advisory Available at http://www.securityfocus.com/bid/93300
Google Android <=7.0 Remote Elevation of Privilege in MediaTek Video Driver	Google Android 7.0 and earlier before 2016-10-05 is prone to an elevation of privileges vulnerability in the MediaTek video driver. The flaw could enable a crafted application to execute arbitrary code within the context of the kernel. AKA Android internal bug A-30030994	Version(s):Google Android 0	Published - October 01, 2016 CVE-2016-3937, CVE-2016-3936 CVSS - 9.3 Vendor's Advisory Available : http://www.securityfocus.com/bid/93334
Google Android 6.0, 6.0.1, 7.0 Remote Elevation of privilege in Lock Settings Service	Google Android versions 6.0, 6.0.1 and 7.0 before 1 October 2016 is prone to a elevation of privilege in the the Lock Settings service. This could enable a crafted application to clear the device PIN or password. AKA Android internal bug A-30003944.	Version(s): Google Pixel C 0 Google Nexus Player 0 Google Nexus 9, 7 (2013), 6P, 6, 5X,Google Nexus 5,Google Android One 0,Google Android 6.0.1 , 7.0, 6.0	Published -October 01, 2016 CVE-2016-3908 CVSS - 9.3 Vendor's Advisory Available at: http://www.securityfocus.com/bid/93290
Google Android <=7.0 on Nexus 6P, Android One Remote Elevation of Privilege in Synaptic Touchscreen Driver	Google Android 7.0 and earlier before 5th October 2016 on Nexus 6P and Android One devices are prone to an elevation of privileges vulnerability in the Synaptic Touchscreen driver. The flaw could enable a crafted application to execute arbitrary code in the context of the kernel. AKA Android internal bug A-30141991.	Version(s): Google Nexus 6P Google Nexus 5X Google Android One 0 Google Android 0	Published -October 01, 2016 CVE-2016-3940,CVE-2016-6672 CVSS - 9.3 Vendor's Advisory Available: http://www.securityfocus.com/bid/93338