Vulnerability Summary for the Week of April 10, 2017

Please Note:

- The vulnerabilities are cattegorized by their level of severity which is either High, Medium or Low.
- The CVE indentity number is the publicly known ID given to that particular vulnerability. Therefore you can search the status of that particular vulnerability using that ID.
- The CVSS (Common Vulnerability Scoring System) score is a standard scoring system used to determine the severity of the vulnerability.

High Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
amazon -- fire_os	Stack-based buffer overflow in the havok_write function in drivers/staging/havok/havok.c in Amazon Fire OS before 2016-01-15 allows attackers to cause a denial of service (panic) or possibly have unspecified other impact via a long string to /dev/hv.	2017-04-09	10.0	CVE-2015-7292 MISC (link is external)
atlassian -- jira	The JIRA Workflow Designer Plugin in Atlassian JIRA Server before 6.3.0 improperly uses an XML parser and deserializer, which allows remote attackers to execute arbitrary code, read arbitrary files, or cause a denial of service via a crafted serialized Java object.	2017-04-10	7.5	CVE-2017-5983 MISC (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CERT-VN
axis -- axis_communications_firmware	AXIS Communications products with firmware through 5.80.x allow remote attackers to modify arbitrary files as root via vectors involving Open Script Editor, aka a "resource injection vulnerability."	2017-04-09	7.8	CVE-2015-8258 EXPLOIT-DB (link is external)

botan_project -- botan	botan before 1.11.22 improperly validates certificate paths, which allows remote attackers to cause a denial of service (infinite loop and memory consumption) via a certificate with a loop in the certificate chain.	2017-04-10	7.8	CVE-2015-7825 CONFIRM (link is external) CONFIRM (link is external)
botan_project -- botan	botan 1.11.x before 1.11.22 improperly handles wildcard matching against hostnames, which might allow remote attackers to have unspecified impact via a valid X.509 certificate, as demonstrated by accepting *.example.com as a match for bar.foo.example.com.	2017-04-10	7.5	CVE-2015-7826 CONFIRM (link is external) CONFIRM (link is external)
botan_project -- botan	The Curve25519 code in botan before 1.11.31, on systems without a native 128-bit integer type, might allow attackers to have unspecified impact via vectors related to undefined behavior, as demonstrated on 32-bit ARM systems compiled by Clang.	2017-04-10	7.5	CVE-2016-6878 CONFIRM (link is external)
cisco -- aironet_access_point	A vulnerability in login authentication management in Cisco Aironet 1800, 2800, and 3800 Series Access Point platforms could allow an authenticated, local attacker to gain unrestricted root access to the underlying Linux operating system. The root Linux shell is provided for advanced troubleshooting and should not be available to individual users, even those with root privileges. The attacker must have the root password to exploit this vulnerability. More Information: CSCvb13893. Known Affected Releases: 8.2(121.0) 8.3(102.0). Known Fixed Releases: 8.4(1.53) 8.4(1.52) 8.3(111.0) 8.3(104.23) 8.2(130.0) 8.2(124.1).	2017-04-07	7.2	CVE-2016-9196 BID (link is external) CONFIRM (link is external)
cisco -- firepower_extensible_operating_system	A vulnerability in the local-mgmt CLI command of the Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to perform a command injection attack. More Information: CSCvb61394 CSCvb86816. Known Affected	2017-04-07	7.2	CVE-2017-6597 BID (link is external) CONFIRM (link is external)

	Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.101) 92.1(1.1658) 2.0(1.115).			
cisco -- firepower_extensible_operating_system	A vulnerability in the debug plug-in functionality of the Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to execute arbitrary commands, aka Privilege Escalation. More Information: CSCvb86725 CSCvb86797. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.105) 92.1(1.1733) 2.1(1.69).	2017-04-07	7.2	CVE-2017-6598 BID (link is external) CONFIRM (link is external)
cisco -- firepower_extensible_operating_system	A vulnerability in the CLI of the Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to perform a command injection attack. More Information: CSCvb61351 CSCvb61637. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.101) 92.1(1.1645) 2.0(1.82) 1.1(4.136.	2017-04-07	7.2	CVE-2017-6600 BID (link is external) CONFIRM (link is external)
cisco -- firepower_management_center	A vulnerability in the detection engine reassembly of Secure Sockets Layer (SSL) packets for Cisco Firepower System Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition because the Snort process consumes a high level of CPU resources. Affected Products: This vulnerability affects Cisco Firepower System Software running software releases 6.0.0, 6.1.0, 6.2.0, or 6.2.1 when the device is configured with an SSL policy that has at least one rule specifying traffic decryption. More Information: CSCvc58563. Known Affected Releases: 6.0.0 6.1.0 6.2.0 6.2.1.	2017-04-07	7.1	CVE-2017-3885 BID (link is external) CONFIRM (link is external)
cisco -- mobility_services_engine	A vulnerability in the CLI command parser of the Cisco Mobility Express 2800 and 3800 Series Wireless LAN Controllers could allow an	2017-04-07	7.2	CVE-2016-9197 BID (link is external) CONFIRM (link

	authenticated, local attacker to obtain access to the underlying operating system shell with root-level privileges. More Information: CSCvb70351. Known Affected Releases: 8.3(102.0).			is external)
cloudviewnms -- cloudview_nms	CloudView NMS before 2.10a has a format string issue exploitable over SNMP.	2017-04-09	7.5	CVE-2016-5074 MISC (link is external)
dataprobe -- ibootbar_firmware	Dataprobe iBootBar (with 2007-09-20 and possibly later released firmware) allows remote attackers to bypass authentication, and conduct power-cycle attacks on connected devices, via a DCRABBIT cookie.	2017-04-07	7.5	CVE-2007-6759 MISC (link is external)
dataprobe -- ibootbar_firmware	Dataprobe iBootBar (with 2007-09-20 and possibly later beta firmware) allows remote attackers to bypass authentication, and conduct power-cycle attacks on connected devices, via a DCCOOKIE cookie.	2017-04-07	7.5	CVE-2007-6760 MISC (link is external)
dell -- integrated_remote_access_controller_firmware	Dell Integrated Remote Access Controller (iDRAC) 7/8 before 2.21.21.21 has a format string issue in racadm getsystinfo.	2017-04-09	7.5	CVE-2015-7271 MISC (link is external) BID (link is external)
dell -- integrated_remote_access_controller_firmware	Dell Integrated Remote Access Controller (iDRAC) 6 before 2.80 and 7/8 before 2.21.21.21 allows attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a long SSH username or input.	2017-04-09	7.5	CVE-2015-7272 MISC (link is external) BID (link is external)
dell -- integrated_remote_access_controller_firmware	Dell Integrated Remote Access Controller (iDRAC) 7/8 before 2.21.21.21 has XXE.	2017-04-09	7.5	CVE-2015-7273 MISC (link is external)
gnu -- binutils	elflink.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has a "member access within null pointer" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an "int main() {return 0;}" program.	2017-04-09	7.5	CVE-2017-7614 MISC
google -- android	A remote code execution vulnerability in libavc	2017-04-07	9.3	CVE-2017-0538 BID (link is

	in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33641588.			external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in libhevc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33864300.	2017-04-07	9.3	CVE-2017-0539 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in libhevc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33966031.	2017-04-07	9.3	CVE-2017-0540 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in sonivox in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34031018.	2017-04-07	9.3	CVE-2017-0541 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in libavc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of	2017-04-07	9.3	CVE-2017-0542 BID (link is external) CONFIRM (link is external) CONFIRM (link

	remote code execution within the context of the Mediaserver process. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33934721.			is external)
google -- android	A remote code execution vulnerability in libavc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34097866.	2017-04-07	9.3	CVE-2017-0543 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in CameraBase could enable a local malicious application to execute arbitrary code. This issue is rated as High because it is a local arbitrary code execution in a privileged process. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-31992879.	2017-04-07	9.3	CVE-2017-0544 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in Audioserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32591350.	2017-04-07	9.3	CVE-2017-0545 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in SurfaceFlinger could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32628763.	2017-04-07	9.3	CVE-2017-0546 BID (link is external) CONFIRM (link is external)

google -- android	A remote denial of service vulnerability in libskia could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 7.0, 7.1.1. Android ID: A-33251605.	2017-04-07	7.1	CVE-2017-0548 BID (link is external) CONFIRM (link is external)
google -- android	A remote denial of service vulnerability in libavc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33818508.	2017-04-07	7.1	CVE-2017-0549 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	A remote denial of service vulnerability in libavc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33933140.	2017-04-07	7.1	CVE-2017-0550 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	A remote denial of service vulnerability in libavc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34097231.	2017-04-07	7.1	CVE-2017-0551 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	A remote denial of service vulnerability in libavc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34097915.	2017-04-07	7.1	CVE-2017-0552 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in libnl could enable a local malicious application to execute arbitrary code within the context of the	2017-04-07	7.6	CVE-2017-0553 BID (link is external) CONFIRM (link

	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.			is external)
google -- android	An elevation of privilege vulnerability in the MediaTek touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: N/A. Android ID: A-30202425. References: M-ALPS02898189.	2017-04-07	9.3	CVE-2017-0562 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in the MediaTek thermal driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A-28175904. References: M-ALPS02696516.	2017-04-07	7.6	CVE-2017-0565 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in the MediaTek camera driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A-28470975. References: M-ALPS02696367.	2017-04-07	7.6	CVE-2017-0566 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in the DTS sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A-33964406.	2017-04-07	7.6	CVE-2017-0578 BID (link is external) CONFIRM (link is external)

gynoii -- gcw-1010	Gynoii has a password of guest for the backdoor guest account and a password of 12345 for the backdoor admin account.	2017-04-09	10.0	CVE-2015-2881 MISC (link is external)
ibaby -- m3s_baby_monitor_firmware	iBaby M3S has a password of admin for the backdoor admin account.	2017-04-09	10.0	CVE-2015-2887 MISC (link is external)
lens_laboratories -- peek-a-view_firmware	Lens Peek-a-View has a password of 2601hx for the backdoor admin account, a password of user for the backdoor user account, and a password of guest for the backdoor guest account.	2017-04-09	10.0	CVE-2015-2885 MISC (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm audio driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-33353700. References: QC-CR#1104067.	2017-04-07	7.6	CVE-2017-0454 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Seemp driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-33353601. References: QC-CR#1102288.	2017-04-07	7.6	CVE-2017-0462 CONFIRM (link is external)
linux -- linux_kernel	A remote code execution vulnerability in the Broadcom Wi-Fi firmware could enable a remote attacker to execute arbitrary code within the context of the Wi-Fi SoC. This issue is rated as Critical due to the possibility of remote code execution in the context of the Wi-Fi SoC. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34199105. References: B-RB#110814.	2017-04-07	10.0	CVE-2017-0561 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the HTC touchscreen driver could enable a local	2017-04-07	9.3	CVE-2017-0563 BID (link is external)

	malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10. Android ID: A-32089409.			CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the kernel ION subsystem could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34276203.	2017-04-07	9.3	CVE-2017-0564 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32125310. References: B-RB#112575.	2017-04-07	7.6	CVE-2017-0567 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34197514. References: B-RB#112600.	2017-04-07	7.6	CVE-2017-0568 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires	2017-04-07	7.6	CVE-2017-0569 BID (link is external) CONFIRM (link is external)

	compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34198729. References: B-RB#110666.			
linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34199963. References: B-RB#110688.	2017-04-07	7.6	CVE-2017-0570 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34203305. References: B-RB#111541.	2017-04-07	7.6	CVE-2017-0571 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-34198931. References: B-RB#112597.	2017-04-07	7.6	CVE-2017-0572 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34469904. References: B-RB#91539.	2017-04-07	7.6	CVE-2017-0573 BID (link is external) CONFIRM (link is external)

linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34624457. References: B-RB#113189.	2017-04-07	7.6	CVE-2017-0574 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32658595. References: QC-CR#1103099.	2017-04-07	7.6	CVE-2017-0575 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm crypto engine driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-33544431. References: QC-CR#1103089.	2017-04-07	7.6	CVE-2017-0576 BID (link is external) MISC (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the HTC touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-33842951.	2017-04-07	7.6	CVE-2017-0577 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm video driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is	2017-04-07	7.6	CVE-2017-0579 BID (link is external) CONFIRM (link is external)

	rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34125463. References: QC-CR#1115406.			
linux -- linux_kernel	An elevation of privilege vulnerability in the Synaptics Touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-34325986.	2017-04-07	7.6	CVE-2017-0580 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Synaptics Touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-34614485.	2017-04-07	7.6	CVE-2017-0581 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the HTC OEM fastboot command could enable a local malicious application to execute arbitrary code within the context of the sensor hub. This issue is rated as Moderate because it first requires exploitation of separate vulnerabilities. Product: Android. Versions: Kernel-3.10. Android ID: A-33178836.	2017-04-07	7.6	CVE-2017-0582 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm CP access driver 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 because of vulnerability specific details which limit the impact of the issue. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32068683. References: QC-CR#1103788.	2017-04-07	7.6	CVE-2017-0583 BID (link is external) CONFIRM (link is external)

linux -- linux_kernel	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.	2017-04-10	7.8	CVE-2017-7618 MISC (link is external) BID (link is external)
news_system_project -- news_system	SQL injection vulnerability in NewsController.php in the News module 5.3.2 and earlier for TYPO3 allows unauthenticated users to execute arbitrary SQL commands via vectors involving overwriteDemand for order and OrderByAllowed.	2017-04-07	7.5	CVE-2017-7581 MISC (link is external)
ninka_project -- ninka	Ninka before 1.3.2 might allow remote attackers to obtain sensitive information, manipulate license compliance scan results, or cause a denial of service (process hang) via a crafted filename.	2017-04-10	7.5	CVE-2017-7239 MLIST (link is external) BID (link is external) CONFIRM (link is external)
osram -- lightify_home	OSRAM SYLVANIA Osram Lightify Home before 2016-07-26 allows remote attackers to execute arbitrary commands via TCP port 4000.	2017-04-09	7.5	CVE-2016-5053 MISC (link is external)
philips -- in.sight_b120\37	Philips In.Sight B120/37 has a password of b120root for the backdoor root account, a password of /ADMIN/ for the backdoor admin account, a password of merlin for the backdoor mg3500 account, a password of M100-4674448 for the backdoor user account, and a password of M100-4674448 for the backdoor admin account.	2017-04-09	10.0	CVE-2015-2882 MISC (link is external)
proxygen_project -- proxygen	The SPDY/2 codec in Facebook Proxygen before 2015-11-09 truncates a certain field to two bytes, which allows hijacking and injection attacks.	2017-04-09	7.5	CVE-2015-7264 MISC (link is external)
schneider-electric -- conext_combox_865-1058_firmware	An issue was discovered in Schneider Electric Conext ComBox, model 865-1058, all firmware versions prior to V3.03 BN 830. A series of rapid requests to the device may cause it to reboot.	2017-04-07	7.8	CVE-2017-6019 CONFIRM (link is external) BID (link is external) MISC
sierrawireless -- aleos_firmware	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 allow Embedded_Ace_Set_Task.cgi command	2017-04-09	7.5	CVE-2016-5065 MISC (link is external)

	injection.			
sierrawireless -- aleos_firmware	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 have weak passwords for admin, rauser, sconsole, and user.	2017-04-09	10.0	CVE-2016-5066 MISC (link is external)
sierrawireless -- aleos_firmware	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 allow Hayes AT command injection.	2017-04-09	9.0	CVE-2016-5067 MISC (link is external)
sierrawireless -- aleos_firmware	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 do not require authentication for Embedded_Ace_Get_Task.cgi requests.	2017-04-09	7.5	CVE-2016-5068 MISC (link is external)
sierrawireless -- aleos_firmware	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 use guessable session tokens, which are in the URL.	2017-04-09	7.5	CVE-2016-5069 MISC (link is external)
sierrawireless -- aleos_firmware	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 execute the management web application as root.	2017-04-09	10.0	CVE-2016-5071 MISC (link is external)
sophos -- cyberoam_cr25ing_utm_firmware	Sophos Cyberoam UTM CR25iNG 10.6.3 MR-5 allows remote authenticated users to bypass intended access restrictions via direct object reference, as demonstrated by a request for Licenseinformation.jsp. This is fixed in 10.6.5.	2017-04-07	9.0	CVE-2016-7786 MISC (link is external)
summer_infant -- baby_zoom_wifi_monitor_firmware	Summer Baby Zoom Wifi Monitor & Internet Viewing System allows remote attackers to bypass authentication, related to the MySnapCam web service.	2017-04-09	7.5	CVE-2015-2888 MISC (link is external)
trendnet -- tv-ip743sic	TRENDnet WiFi Baby Cam TV-IP743SIC has a password of admin for the backdoor root account.	2017-04-09	9.0	CVE-2015-2880 MISC (link is external)
vertivco -- liebert_multilink_automated_shutdown	Liebert MultiLink Automated Shutdown v4.2.4 allows local users to gain privileges by replacing the LiebertM executable file.	2017-04-09	7.2	CVE-2015-7260 MISC (link is external)
amazon -- fire_os	Stack-based buffer overflow in the havok_write function in drivers/staging/havok/havok.c in Amazon Fire OS before 2016-01-15 allows attackers to cause a denial of service (panic) or possibly have unspecified other impact via a long string to /dev/hv.	2017-04-09	10.0	CVE-2015-7292 MISC (link is external)

atlassian -- jira	The JIRA Workflow Designer Plugin in Atlassian JIRA Server before 6.3.0 improperly uses an XML parser and deserializer, which allows remote attackers to execute arbitrary code, read arbitrary files, or cause a denial of service via a crafted serialized Java object.	2017-04-10	7.5	CVE-2017-5983 MISC (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CERT-VN
axis -- axis_communications_firmware	AXIS Communications products with firmware through 5.80.x allow remote attackers to modify arbitrary files as root via vectors involving Open Script Editor, aka a "resource injection vulnerability."	2017-04-09	7.8	CVE-2015-8258 EXPLOIT-DB (link is external)
botan_project -- botan	botan before 1.11.22 improperly validates certificate paths, which allows remote attackers to cause a denial of service (infinite loop and memory consumption) via a certificate with a loop in the certificate chain.	2017-04-10	7.8	CVE-2015-7825 CONFIRM (link is external) CONFIRM (link is external)
botan_project -- botan	botan 1.11.x before 1.11.22 improperly handles wildcard matching against hostnames, which might allow remote attackers to have unspecified impact via a valid X.509 certificate, as demonstrated by accepting *.example.com as a match for bar.foo.example.com.	2017-04-10	7.5	CVE-2015-7826 CONFIRM (link is external) CONFIRM (link is external)
botan_project -- botan	The Curve25519 code in botan before 1.11.31, on systems without a native 128-bit integer type, might allow attackers to have unspecified impact via vectors related to undefined behavior, as demonstrated on 32-bit ARM systems compiled by Clang.	2017-04-10	7.5	CVE-2016-6878 CONFIRM (link is external)
cisco -- aironet_access_point	A vulnerability in login authentication management in Cisco Aironet 1800, 2800, and 3800 Series Access Point platforms could allow an authenticated, local attacker to gain unrestricted root access to the underlying Linux operating system. The root Linux shell is provided for advanced troubleshooting and should not be available to individual users, even those with root privileges. The attacker must	2017-04-07	7.2	CVE-2016-9196 BID (link is external) CONFIRM (link is external)

	have the root password to exploit this vulnerability. More Information: CSCvb13893. Known Affected Releases: 8.2(121.0) 8.3(102.0). Known Fixed Releases: 8.4(1.53) 8.4(1.52) 8.3(111.0) 8.3(104.23) 8.2(130.0) 8.2(124.1).			
cisco -- firepower_extensible_operating_system	A vulnerability in the local-mgmt CLI command of the Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to perform a command injection attack. More Information: CSCvb61394 CSCvb86816. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.101) 92.1(1.1658) 2.0(1.115).	2017-04-07	7.2	CVE-2017-6597 BID (link is external) CONFIRM (link is external)
cisco -- firepower_extensible_operating_system	A vulnerability in the debug plug-in functionality of the Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to execute arbitrary commands, aka Privilege Escalation. More Information: CSCvb86725 CSCvb86797. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.105) 92.1(1.1733) 2.1(1.69).	2017-04-07	7.2	CVE-2017-6598 BID (link is external) CONFIRM (link is external)
cisco -- firepower_extensible_operating_system	A vulnerability in the CLI of the Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to perform a command injection attack. More Information: CSCvb61351 CSCvb61637. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.101) 92.1(1.1645) 2.0(1.82) 1.1(4.136.	2017-04-07	7.2	CVE-2017-6600 BID (link is external) CONFIRM (link is external)
cisco -- firepower_management_center	A vulnerability in the detection engine reassembly of Secure Sockets Layer (SSL) packets for Cisco Firepower System Software could allow	2017-04-07	7.1	CVE-2017-3885 BID (link is external) CONFIRM (link

	an unauthenticated, remote attacker to cause a denial of service (DoS) condition because the Snort process consumes a high level of CPU resources. Affected Products: This vulnerability affects Cisco Firepower System Software running software releases 6.0.0, 6.1.0, 6.2.0, or 6.2.1 when the device is configured with an SSL policy that has at least one rule specifying traffic decryption. More Information: CSCvc58563. Known Affected Releases: 6.0.0 6.1.0 6.2.0 6.2.1.			is external)
cisco -- mobility_services_engine	A vulnerability in the CLI command parser of the Cisco Mobility Express 2800 and 3800 Series Wireless LAN Controllers could allow an authenticated, local attacker to obtain access to the underlying operating system shell with root-level privileges. More Information: CSCvb70351. Known Affected Releases: 8.3(102.0).	2017-04-07	7.2	CVE-2016-9197 BID (link is external) CONFIRM (link is external)
cloudviewnms -- cloudview_nms	CloudView NMS before 2.10a has a format string issue exploitable over SNMP.	2017-04-09	7.5	CVE-2016-5074 MISC (link is external)
dataprobe -- ibootbar_firmware	Dataprobe iBootBar (with 2007-09-20 and possibly later released firmware) allows remote attackers to bypass authentication, and conduct power-cycle attacks on connected devices, via a DCRABBIT cookie.	2017-04-07	7.5	CVE-2007-6759 MISC (link is external)
dataprobe -- ibootbar_firmware	Dataprobe iBootBar (with 2007-09-20 and possibly later beta firmware) allows remote attackers to bypass authentication, and conduct power-cycle attacks on connected devices, via a DCCOOKIE cookie.	2017-04-07	7.5	CVE-2007-6760 MISC (link is external)
dell -- integrated_remote_access_controller_firmware	Dell Integrated Remote Access Controller (iDRAC) 7/8 before 2.21.21.21 has a format string issue in racadm getsystinfo.	2017-04-09	7.5	CVE-2015-7271 MISC (link is external) BID (link is external)
dell -- integrated_remote_access_controller_firmware	Dell Integrated Remote Access Controller (iDRAC) 6 before 2.80 and 7/8 before 2.21.21.21 allows attackers to cause a denial of service (buffer overflow) or possibly have unspecified other impact via a long SSH username or input.	2017-04-09	7.5	CVE-2015-7272 MISC (link is external) BID (link is external)

dell -- integrated_remote_access_controller_firmware	Dell Integrated Remote Access Controller (iDRAC) 7/8 before 2.21.21.21 has XXE.	2017-04-09	7.5	CVE-2015-7273 MISC (link is external)
gnu -- binutils	elflink.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.28, has a "member access within null pointer" undefined behavior issue, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an "int main() {return 0;}" program.	2017-04-09	7.5	CVE-2017-7614 MISC
google -- android	A remote code execution vulnerability in libavc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33641588.	2017-04-07	9.3	CVE-2017-0538 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in libhevc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33864300.	2017-04-07	9.3	CVE-2017-0539 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in libhevc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33966031.	2017-04-07	9.3	CVE-2017-0540 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in sonivox	2017-04-07	9.3	CVE-2017-0541 BID (link is

	in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34031018.			external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in libavc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33934721.	2017-04-07	9.3	CVE-2017-0542 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in libavc in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34097866.	2017-04-07	9.3	CVE-2017-0543 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in CameraBase could enable a local malicious application to execute arbitrary code. This issue is rated as High because it is a local arbitrary code execution in a privileged process. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-31992879.	2017-04-07	9.3	CVE-2017-0544 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in Audioserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 5.0.2,	2017-04-07	9.3	CVE-2017-0545 BID (link is external) CONFIRM (link is external)

	5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32591350.			
google -- android	An elevation of privilege vulnerability in SurfaceFlinger could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32628763.	2017-04-07	9.3	CVE-2017-0546 BID (link is external) CONFIRM (link is external)
google -- android	A remote denial of service vulnerability in libskia could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 7.0, 7.1.1. Android ID: A-33251605.	2017-04-07	7.1	CVE-2017-0548 BID (link is external) CONFIRM (link is external)
google -- android	A remote denial of service vulnerability in libavc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33818508.	2017-04-07	7.1	CVE-2017-0549 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	A remote denial of service vulnerability in libavc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33933140.	2017-04-07	7.1	CVE-2017-0550 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	A remote denial of service vulnerability in libavc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service.	2017-04-07	7.1	CVE-2017-0551 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)

	Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34097231.			CONFIRM (link is external)
google -- android	A remote denial of service vulnerability in libavc in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as High severity due to the possibility of remote denial of service. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34097915.	2017-04-07	7.1	CVE-2017-0552 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	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.	2017-04-07	7.6	CVE-2017-0553 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in the MediaTek touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: N/A. Android ID: A-30202425. References: M-ALPS02898189.	2017-04-07	9.3	CVE-2017-0562 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in the MediaTek thermal driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A-28175904. References: M-ALPS02696516.	2017-04-07	7.6	CVE-2017-0565 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in the MediaTek camera driver could enable a local	2017-04-07	7.6	CVE-2017-0566 BID (link is external)

	malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A-28470975. References: M-ALPS02696367.			CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in the DTS sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: N/A. Android ID: A-33964406.	2017-04-07	7.6	CVE-2017-0578 BID (link is external) CONFIRM (link is external)
gynoii -- gcw-1010	Gynoii has a password of guest for the backdoor guest account and a password of 12345 for the backdoor admin account.	2017-04-09	10.0	CVE-2015-2881 MISC (link is external)
ibaby -- m3s_baby_monitor_firmware	iBaby M3S has a password of admin for the backdoor admin account.	2017-04-09	10.0	CVE-2015-2887 MISC (link is external)
lens_laboratories -- peek-a-view_firmware	Lens Peek-a-View has a password of 2601hx for the backdoor admin account, a password of user for the backdoor user account, and a password of guest for the backdoor guest account.	2017-04-09	10.0	CVE-2015-2885 MISC (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm audio driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-33353700. References: QC-CR#1104067.	2017-04-07	7.6	CVE-2017-0454 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Seemp driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product:	2017-04-07	7.6	CVE-2017-0462 CONFIRM (link is external)

	Android. Versions: Kernel-3.18. Android ID: A-33353601. References: QC-CR#1102288.			
linux -- linux_kernel	A remote code execution vulnerability in the Broadcom Wi-Fi firmware could enable a remote attacker to execute arbitrary code within the context of the Wi-Fi SoC. This issue is rated as Critical due to the possibility of remote code execution in the context of the Wi-Fi SoC. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34199105. References: B-RB#110814.	2017-04-07	10.0	CVE-2017-0561 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the HTC touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10. Android ID: A-32089409.	2017-04-07	9.3	CVE-2017-0563 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the kernel ION subsystem could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34276203.	2017-04-07	9.3	CVE-2017-0564 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32125310. References: B-RB#112575.	2017-04-07	7.6	CVE-2017-0567 BID (link is external) CONFIRM (link is external)

linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34197514. References: B-RB#112600.	2017-04-07	7.6	CVE-2017-0568 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34198729. References: B-RB#110666.	2017-04-07	7.6	CVE-2017-0569 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34199963. References: B-RB#110688.	2017-04-07	7.6	CVE-2017-0570 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34203305. References: B-RB#111541.	2017-04-07	7.6	CVE-2017-0571 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code	2017-04-07	7.6	CVE-2017-0572 BID (link is external) CONFIRM (link

	within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-34198931. References: B-RB#112597.			is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34469904. References: B-RB#91539.	2017-04-07	7.6	CVE-2017-0573 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34624457. References: B-RB#113189.	2017-04-07	7.6	CVE-2017-0574 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32658595. References: QC-CR#1103099.	2017-04-07	7.6	CVE-2017-0575 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm crypto engine driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18.	2017-04-07	7.6	CVE-2017-0576 BID (link is external) MISC (link is external) CONFIRM (link is external)

	Android ID: A-33544431. References: QC-CR#1103089.			
linux -- linux_kernel	An elevation of privilege vulnerability in the HTC touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-33842951.	2017-04-07	7.6	CVE-2017-0577 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm video driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-34125463. References: QC-CR#1115406.	2017-04-07	7.6	CVE-2017-0579 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Synaptics Touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-34325986.	2017-04-07	7.6	CVE-2017-0580 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Synaptics Touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-34614485.	2017-04-07	7.6	CVE-2017-0581 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the HTC OEM fastboot command could enable a local malicious application to execute arbitrary code	2017-04-07	7.6	CVE-2017-0582 BID (link is external) CONFIRM (link

	within the context of the sensor hub. This issue is rated as Moderate because it first requires exploitation of separate vulnerabilities. Product: Android. Versions: Kernel-3.10. Android ID: A-33178836.			is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm CP access driver 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 because of vulnerability specific details which limit the impact of the issue. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32068683. References: QC-CR#1103788.	2017-04-07	7.6	CVE-2017-0583 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	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.	2017-04-10	7.8	CVE-2017-7618 MISC (link is external) BID (link is external)
news_system_project -- news_system	SQL injection vulnerability in NewsController.php in the News module 5.3.2 and earlier for TYPO3 allows unauthenticated users to execute arbitrary SQL commands via vectors involving overwriteDemand for order and OrderByAllowed.	2017-04-07	7.5	CVE-2017-7581 MISC (link is external)
ninka_project -- ninka	Ninka before 1.3.2 might allow remote attackers to obtain sensitive information, manipulate license compliance scan results, or cause a denial of service (process hang) via a crafted filename.	2017-04-10	7.5	CVE-2017-7239 MLIST (link is external) BID (link is external) CONFIRM (link is external)
osram -- lightify_home	OSRAM SYLVANIA Osram Lightify Home before 2016-07-26 allows remote attackers to execute arbitrary commands via TCP port 4000.	2017-04-09	7.5	CVE-2016-5053 MISC (link is external)
philips -- in.sight_b120\37	Philips In.Sight B120/37 has a password of b120root for the backdoor root account, a password of /ADMIN/ for the backdoor admin account, a password of merlin for the backdoor	2017-04-09	10.0	CVE-2015-2882 MISC (link is external)

	mg3500 account, a password of M100-4674448 for the backdoor user account, and a password of M100-4674448 for the backdoor admin account.			
proxygen_project -- proxygen	The SPDY/2 codec in Facebook Proxygen before 2015-11-09 truncates a certain field to two bytes, which allows hijacking and injection attacks.	2017-04-09	7.5	CVE-2015-7264 MISC (link is external)
schneider-electric -- conext_combox_865-1058_firmware	An issue was discovered in Schneider Electric Conext ComBox, model 865-1058, all firmware versions prior to V3.03 BN 830. A series of rapid requests to the device may cause it to reboot.	2017-04-07	7.8	CVE-2017-6019 CONFIRM (link is external) BID (link is external) MISC
sierrawireless -- aleos_firmware	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 allow Embedded_Ace_Set_Task.cgi command injection.	2017-04-09	7.5	CVE-2016-5065 MISC (link is external)
sierrawireless -- aleos_firmware	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 have weak passwords for admin, rauser, sconsole, and user.	2017-04-09	10.0	CVE-2016-5066 MISC (link is external)
sierrawireless -- aleos_firmware	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 allow Hayes AT command injection.	2017-04-09	9.0	CVE-2016-5067 MISC (link is external)
sierrawireless -- aleos_firmware	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 do not require authentication for Embedded_Ace_Get_Task.cgi requests.	2017-04-09	7.5	CVE-2016-5068 MISC (link is external)
sierrawireless -- aleos_firmware	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 use guessable session tokens, which are in the URL.	2017-04-09	7.5	CVE-2016-5069 MISC (link is external)
sierrawireless -- aleos_firmware	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 execute the management web application as root.	2017-04-09	10.0	CVE-2016-5071 MISC (link is external)
sophos -- cyberoam_cr25ing_utm_firmware	Sophos Cyberoam UTM CR25iNG 10.6.3 MR-5 allows remote authenticated users to bypass intended access restrictions via direct object reference, as demonstrated by a request for Licenseinformation.jsp. This is fixed in 10.6.5.	2017-04-07	9.0	CVE-2016-7786 MISC (link is external)
summer_infant --	Summer Baby Zoom Wifi Monitor & Internet	2017-04-09	7.5	CVE-2015-2888 MISC (link is

baby_zoom_wifi_monitor_firmware	Viewing System allows remote attackers to bypass authentication, related to the MySnapCam web service.			external)
trendnet -- tv-ip743sic	TRENDnet WiFi Baby Cam TV-IP743SIC has a password of admin for the backdoor root account.	2017-04-09	9.0	CVE-2015-2880 MISC (link is external)
vertivco -- liebert_multilink_automated_shutdown	Liebert MultiLink Automated Shutdown v4.2.4 allows local users to gain privileges by replacing the LiebertM executable file.	2017-04-09	7.2	CVE-2015-7260 MISC (link is external)

Medium Severity Vulnerabilities

The Primary Vendor --- Product	Description	Date Published	CVSS Score	The CVE Identity
apache -- ignite	Apache Ignite before 1.9 allows man-in-the-middle attackers to read arbitrary files via XXE in modified update-notifier documents.	2017-04-07	4.3	CVE-2016-6805 CONFIRM BID (link is external)
atlassian -- bitbucket	Atlassian Bitbucket Server before 4.7.1 allows remote attackers to read the first line of an arbitrary file via a directory traversal attack on the pull requests resource.	2017-04-09	4.0	CVE-2016-4320 BID (link is external) MISC (link is external)
atlassian -- jira	Atlassian JIRA Server before 7.1.9 has CSRF in auditing/settings.	2017-04-09	6.8	CVE-2016-4319 BID (link is external) MISC (link is external)
axis -- axis_communications_firmware	AXIS Communications products allow CSRF, as demonstrated by admin/pwdgrp.cgi, vaconfig.cgi, and admin/local_del.cgi.	2017-04-09	6.8	CVE-2015-8255 EXPLOIT-DB (link is external)
botan_project -- botan	botan 1.11.x before 1.11.22 makes it easier for remote attackers to decrypt TLS ciphertext data via a padding-oracle attack against TLS CBC	2017-04-10	5.0	CVE-2015-7824 CONFIRM (link is external) CONFIRM (link

	ciphersuites.			is external)
botan_project -- botan	The X509_Certificate::allowed_usage function in botan 1.11.x before 1.11.31 might allow attackers to have unspecified impact by leveraging a call with more than one Key_Usage set in the enum value.	2017-04-10	5.0	CVE-2016-6879 CONFIRM (link is external)
castle_rock_computing -- snmpc	Castle Rock Computing SNMPc before 2015-12-17 has XSS via SNMP.	2017-04-09	4.3	CVE-2015-6027 MISC (link is external)
castle_rock_computing -- snmpc	Castle Rock Computing SNMPc before 2015-12-17 has SQL injection via the sc parameter.	2017-04-09	6.5	CVE-2015-6028 MISC (link is external)
cesanta -- mongoose_os	Use-after-free vulnerability in the mg_http_multipart_wait_for_boundary function in mongoose.c in Cesanta Mongoose Embedded Web Server Library 6.7 and earlier and Mongoose OS 1.2 and earlier allows remote attackers to cause a denial of service (crash) via a multipart/form-data POST request without a MIME boundary string.	2017-04-10	5.0	CVE-2017-7185 BUGTRAQ (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) MISC (link is external)
cisco -- asr_900_series_firmware	A vulnerability in Cisco ASR 903 or ASR 920 Series Devices running with an RSP2 card could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on a targeted system because of incorrect IPv6 Packet Processing. More Information: CSCuy94366. Known Affected Releases: 15.4(3)S3.15. Known Fixed Releases: 15.6(2)SP 15.6(1.31)SP.	2017-04-07	6.1	CVE-2017-6603 BID (link is external) CONFIRM (link is external)
cisco -- firepower_threat_defense	A vulnerability in the detection engine that handles Secure Sockets Layer (SSL) packets for Cisco Firepower System Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition because the Snort process unexpectedly restarts. This vulnerability affects Cisco Firepower System Software prior to the first fixed release when it is configured with an SSL Decrypt-Resign policy. More Information: CSCvb62292. Known Affected Releases: 6.0.1 6.1.0 6.2.0. Known Fixed Releases: 6.2.0 6.1.0.2.	2017-04-07	4.3	CVE-2017-3887 BID (link is external) CONFIRM (link is external)
cisco -- ios_xe	A vulnerability in a startup script of Cisco IOS XE	2017-04-07	6.9	CVE-2017-6606

	Software could allow an unauthenticated attacker with physical access to the targeted system to execute arbitrary commands on the underlying operating system with the privileges of the root user. More Information: CSCuz06639 CSCuz42122. Known Affected Releases: 15.6(1.1)S 16.1.2 16.2.0 15.2(1)E. Known Fixed Releases: Denali-16.1.3 16.2(1.8) 16.1(2.61) 15.6(2)SP 15.6(2)S1 15.6(1)S2 15.5(3)S3a 15.5(3)S3 15.5(2)S4 15.5(1)S4 15.4(3)S6a 15.4(3)S6 15.3(3)S8a 15.3(3)S8 15.2(5)E 15.2(4)E3 15.2(3)E5 15.0(2)SQD3 15.0(1.9.2)SQD3 3.9(0)E.			BID (link is external) CONFIRM (link is external)
cisco -- ios_xr	A vulnerability in Google-defined remote procedure call (gRPC) handling in Cisco IOS XR Software could allow an unauthenticated, remote attacker to cause the Event Management Service daemon (emsd) to crash due to a system memory leak, resulting in a denial of service (DoS) condition. This vulnerability affects Cisco IOS XR Software with gRPC enabled. More Information: CSCvb14433. Known Affected Releases: 6.1.1.BASE 6.2.1.BASE. Known Fixed Releases: 6.2.1.22i.MGBL 6.1.22.9i.MGBL 6.1.21.12i.MGBL 6.1.2.13i.MGBL.	2017-04-07	5.0	CVE-2017-6599 BID (link is external) CONFIRM (link is external)
cisco -- prime_infrastructure	A vulnerability in the HTTP web-based management interface of Cisco Prime Infrastructure could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the web interface of the affected system. More Information: CSCuw63001 CSCuw63003. Known Affected Releases: 2.2(2). Known Fixed Releases: 3.1(0.0).	2017-04-07	4.3	CVE-2017-3848 BID (link is external) CONFIRM (link is external)
cisco -- prime_infrastructure	A vulnerability in the web interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network (EPN) Manager could allow an authenticated, remote attacker to access sensitive data. The attacker does not need administrator credentials and could use this information to conduct additional reconnaissance attacks. More Information: CSCvc60031 (Fixed) CSCvc60041 (Fixed) CSCvc60095 (Open) CSCvc60102 (Open).	2017-04-07	4.0	CVE-2017-3884 BID (link is external) CONFIRM (link is external)

	Known Affected Releases: 2.2 2.2(3) 3.0 3.1(0.0) 3.1(0.128) 3.1(4.0) 3.1(5.0) 3.2(0.0) 2.0(4.0.45D).			
cisco -- registered_envelope_service	A vulnerability in the web interface of the Cisco Registered Envelope Service could allow an unauthenticated, remote attacker to redirect a user to a undesired web page, aka an Open Redirect. This vulnerability affects the Cisco Registered Envelope cloud-based service. More Information: CSCvc60123. Known Affected Releases: 5.1.0-015.	2017-04-07	5.8	CVE-2017-3889 BID (link is external) CONFIRM (link is external)
cisco -- unified_communications_manager	A vulnerability in the Cisco Unified Communications Manager web interface could allow an authenticated, remote attacker to impact the confidentiality of the system by executing arbitrary SQL queries, aka SQL Injection. The attacker must be authenticated as an administrative user to execute SQL database queries. More Information: CSCvc74291. Known Affected Releases: 1.0(1.10000.10) 11.5(1.10000.6). Known Fixed Releases: 12.0(0.98000.619) 12.0(0.98000.485) 12.0(0.98000.212) 11.5(1.13035.1) 11.0(1.23900.5) 11.0(1.23900.2) 11.0(1.23067.1) 10.5(2.15900.2).	2017-04-07	4.0	CVE-2017-3886 BID (link is external) CONFIRM (link is external)
cisco -- unified_computing_system	A vulnerability in the web interface of Cisco Integrated Management Controller (IMC) Software could allow an unauthenticated, remote attacker to redirect a user to a malicious web page. This vulnerability affects the following Cisco products running Cisco IMC Software: Unified Computing System (UCS) B-Series M3 and M4 Blade Servers, Unified Computing System (UCS) C-Series M3 and M4 Rack Servers. More Information: CSCvc37931. Known Affected Releases: 3.1(2c)B.	2017-04-07	5.8	CVE-2017-6604 BID (link is external) CONFIRM (link is external)
cisco -- unified_computing_system_director	A vulnerability in the role-based resource checking functionality of Cisco Unified Computing System (UCS) Director could allow an authenticated, remote attacker to view unauthorized information for any virtual machine in a UCS domain. More Information: CSCvc32434. Known Affected Releases: 5.5(0.1) 6.0(0.0).	2017-04-07	4.0	CVE-2017-3817 BID (link is external) CONFIRM (link is external)

cisco -- wireless_lan_controller	A vulnerability in RADIUS Change of Authorization (CoA) request processing in the Cisco Wireless LAN Controller (WLC) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition by disconnecting a single connection. This vulnerability affects Cisco Wireless LAN Controller running software release 8.3.102.0. More Information: CSCvb01835. Known Fixed Releases: 8.4(1.49) 8.3(111.0) 8.3(108.0) 8.3(104.24) 8.3(102.3).	2017-04-07	5.0	CVE-2016-9195 BID (link is external) CONFIRM (link is external)
cloudera -- cdh	Impala in CDH 5.2.0 through 5.7.2 and 5.8.0 allows remote attackers to bypass Setry authorization.	2017-04-10	5.0	CVE-2016-6605 CONFIRM (link is external)
cloudviewnms -- cloudview_nms	CloudView NMS before 2.10a has XSS via SNMP.	2017-04-09	4.3	CVE-2016-5073 MISC (link is external)
cloudviewnms -- cloudview_nms	CloudView NMS before 2.10a has XSS via a TELNET login.	2017-04-09	4.3	CVE-2016-5075 MISC (link is external)
cloudviewnms -- cloudview_nms	CloudView NMS before 2.10a allows remote attackers to obtain sensitive information via a direct request for admin/auto.def.	2017-04-09	5.0	CVE-2016-5076 MISC (link is external)
dell -- integrated_remote_access_controller_firmware	Dell Integrated Remote Access Controller (iDRAC) 6 before 2.80 and 7/8 before 2.21.21.21 allows directory traversal.	2017-04-09	4.6	CVE-2015-7270 MISC (link is external) BID (link is external)
dell -- integrated_remote_access_controller_firmware	Dell Integrated Remote Access Controller (iDRAC) 6 before 2.80 allows remote attackers to execute arbitrary administrative HTTP commands.	2017-04-09	6.5	CVE-2015-7274 MISC (link is external) BID (link is external) BID (link is external)
dell -- integrated_remote_access_controller_firmware	Dell Integrated Remote Access Controller (iDRAC) 6 before 2.85 and 7/8 before 2.30.30.30 has XSS.	2017-04-09	4.3	CVE-2015-7275 MISC (link is external) BID (link is external)
dlink -- dwr-116_firmware	Directory traversal vulnerability in the web interface on the D-Link DWR-116 device with firmware before V1.05b09 allows remote attackers to read arbitrary files via a .. (dot dot) in a "GET /uir/"	2017-04-10	5.0	CVE-2017-6190 BID (link is external) MISC (link is external)

	request.			
elfutils_project -- elfutils	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.	2017-04-09	4.3	CVE-2017-7607 MISC
elfutils_project -- elfutils	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.	2017-04-09	4.3	CVE-2017-7608 MISC
elfutils_project -- elfutils	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.	2017-04-09	4.3	CVE-2017-7609 MISC
elfutils_project -- elfutils	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.	2017-04-09	4.3	CVE-2017-7610 MISC
elfutils_project -- elfutils	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.	2017-04-09	4.3	CVE-2017-7611 MISC
elfutils_project -- elfutils	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.	2017-04-09	4.3	CVE-2017-7612 MISC
elfutils_project -- elfutils	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.	2017-04-09	4.3	CVE-2017-7613 MISC
eparaksts -- eparakstitajs_3	LVRTC eParakstitajs 3.0 (1.3.0) and edoc-libraries-2.5.4_01 allow attackers to write to arbitrary files via crafted EDOC files.	2017-04-09	4.3	CVE-2015-8275 MISC (link is external)
eparaksts -- eparakstitajs_3	LVRTC eParakstitajs 3.0 (1.3.0) and edoc-libraries-2.5.4_01 allow attackers to read arbitrary files via crafted EDOC files.	2017-04-09	4.3	CVE-2015-8276 MISC (link is external)
foxitsoftware --	Memory Corruption Vulnerability in Foxit PDF	2017-04-07	6.8	CVE-2017-7584

foxit_pdf_toolkit	Toolkit before 2.1 allows an attacker to cause Denial of Service & Remote Code Execution when a victim opens a specially crafted PDF file.			BID (link is external) CONFIRM (link is external)
google -- android	An information disclosure vulnerability in libmedia in Mediaserver could enable a local malicious application to access data outside of its permission levels. This issue is rated as High because it is a general bypass for operating system protections that isolate application data from other applications. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33861560.	2017-04-07	4.3	CVE-2017-0547 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in the Telephony component could enable a local malicious application to access capabilities outside of its permission levels. This issue is rated as Moderate because it could be used to gain access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33815946.	2017-04-07	6.8	CVE-2017-0554 BID (link is external) CONFIRM (link is external)
google -- android	An information disclosure vulnerability in libavc in Mediaserver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access data without permission. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33551775.	2017-04-07	4.3	CVE-2017-0555 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	An information disclosure vulnerability in libmpeg2 in Mediaserver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access data without permission. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34093952.	2017-04-07	4.3	CVE-2017-0556 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	An information disclosure vulnerability in libmpeg2 in Mediaserver could enable a local malicious application to access data outside of its permission	2017-04-07	4.3	CVE-2017-0557 BID (link is external) CONFIRM (link

	levels. This issue is rated as Moderate because it could be used to access data without permission. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34093073.			is external) CONFIRM (link is external)
google -- android	An information disclosure vulnerability in Mediaserver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access data without permission. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-34056274.	2017-04-07	4.3	CVE-2017-0558 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
google -- android	An information disclosure vulnerability in libskia could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access data without permission. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33897722.	2017-04-07	4.3	CVE-2017-0559 BID (link is external) CONFIRM (link is external)
google -- android	An information disclosure vulnerability in the factory reset process could enable a local malicious attacker to access data from the previous owner. This issue is rated as Moderate due to the possibility of bypassing device protection. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-30681079.	2017-04-07	4.3	CVE-2017-0560 BID (link is external) CONFIRM (link is external)
ibaby -- m6_baby_monitor_firmware	iBaby M6 allows remote attackers to obtain sensitive information, related to the ibabycloud.com service.	2017-04-09	5.0	CVE-2015-2886 MISC (link is external)
ilias_project -- ilias	ILIAS before 5.2.3 has XSS via SVG documents.	2017-04-07	4.3	CVE-2017-7583 CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	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	2017-04-09	4.3	CVE-2017-7606 MISC

	other impact via a crafted image.			
imagemagick -- imagemagick	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.	2017-04-10	5.0	CVE-2017-7619 CONFIRM
imageworsener_project -- imageworsener	The iwmiffr_convert_row32 function in imagew-miff.c in libimageworsener.a in ImageWorsener 1.3.0 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted file.	2017-04-10	4.3	CVE-2017-7623 BID (link is external) CONFIRM (link is external)
imageworsener_project -- imageworsener	The iw_read_bmp_file function in imagew-bmp.c in libimageworsener.a in ImageWorsener 1.3.0 allows remote attackers to consume an amount of available memory via a crafted file.	2017-04-10	4.3	CVE-2017-7624 BID (link is external) CONFIRM (link is external)
jive_software -- jive	Jive before 2016.3.1 has an open redirect from the external-link.jspa page.	2017-04-09	5.8	CVE-2016-4334 MISC (link is external)
keepassx_project -- keepassx	In KeePassX before 0.4.4, a cleartext copy of password data is created upon a cancel of an XML export action. This allows context-dependent attackers to obtain sensitive information by reading the .xml dotfile.	2017-04-10	5.0	CVE-2015-8378 CONFIRM CONFIRM
libaacplus_project -- libaacplus	au_channel.h in HE-AAC+ Codec (aka libaacplus) 2.0.2 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 audio file.	2017-04-09	6.8	CVE-2017-7603 MISC
libaacplus_project -- libaacplus	au_channel.h in HE-AAC+ Codec (aka libaacplus) 2.0.2 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 audio file.	2017-04-09	6.8	CVE-2017-7604 MISC
libaacplus_project -- libaacplus	aacplusenc.c in HE-AAC+ Codec (aka libaacplus) 2.0.2 has an assertion failure, which might allow remote attackers to cause a denial of service (application crash) or possibly have unspecified	2017-04-09	6.8	CVE-2017-7605 MISC

	other impact via a crafted audio file.			
libming -- libming	Multiple heap-based buffer overflows in parser.c in libming 0.4.7 allow remote attackers to cause a denial of service (listswf application crash) or possibly have unspecified other impact via a crafted SWF file. NOTE: this issue exists because of an incomplete fix for CVE-2016-9831.	2017-04-07	6.8	CVE-2017-7578 CONFIRM (link is external)
libsndfile_project -- libsndfile	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.	2017-04-07	4.3	CVE-2017-7585 CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) MISC (link is external)
libsndfile_project -- libsndfile	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.	2017-04-07	4.3	CVE-2017-7586 CONFIRM (link is external) CONFIRM (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
libtiff -- libtiff	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.	2017-04-09	6.8	CVE-2017-7592 MISC BID (link is external)
libtiff -- libtiff	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.	2017-04-09	4.3	CVE-2017-7593 MISC BID (link is external)
libtiff -- libtiff	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.	2017-04-09	4.3	CVE-2017-7594 MISC BID (link is external)
libtiff -- libtiff	The JPEGSetupEncode function in tiff_jpeg.c in	2017-04-09	4.3	CVE-2017-7595 MISC

	LibTIFF 4.0.7 allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted image.			
libtiff -- libtiff	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.	2017-04-09	6.8	CVE-2017-7596 BID (link is external) MISC
libtiff -- libtiff	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.	2017-04-09	6.8	CVE-2017-7597 BID (link is external) MISC
libtiff -- libtiff	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.	2017-04-09	4.3	CVE-2017-7598 BID (link is external) MISC
libtiff -- libtiff	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.	2017-04-09	6.8	CVE-2017-7599 BID (link is external) BID (link is external) MISC
libtiff -- libtiff	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.	2017-04-09	6.8	CVE-2017-7600 MISC
libtiff -- libtiff	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.	2017-04-09	6.8	CVE-2017-7601 BID (link is external) MISC
libtiff -- libtiff	LibTIFF 4.0.7 has a signed integer overflow, which might allow remote attackers to cause a denial of	2017-04-09	6.8	CVE-2017-7602 BID (link is

	service (application crash) or possibly have unspecified other impact via a crafted image.			external) MISC
netapp -- clustered_data_ontap	NetApp Clustered Data ONTAP 8.1 through 9.1P1, when NFS or SMB is enabled, allows remote attackers to cause a denial of service via unspecified vectors.	2017-04-10	5.0	CVE-2017-5988 CONFIRM (link is external)
netikus -- eventsentry	Netikus EventSentry before 3.2.1.44 has XSS via SNMP.	2017-04-09	4.3	CVE-2016-5077 MISC (link is external)
opencv -- opencv	OpenCV 3.0.0 has a double free issue that allows attackers to execute arbitrary code.	2017-04-09	6.8	CVE-2016-1516 MISC MISC (link is external)
opencv -- opencv	OpenCV 3.0.0 allows remote attackers to cause a denial of service (segfault) via vectors involving corrupt chunks.	2017-04-09	4.3	CVE-2016-1517 MISC MISC (link is external)
openidm_project -- openidm	In OpenIDM through 4.0.0 before 4.5.0, the info endpoint may leak sensitive information upon a request by the "anonymous" user, as demonstrated by responses with a 200 HTTP status code and a JSON object containing IP address strings. This is related to a missing access-control check in bin/defaults/script/info/login.js.	2017-04-08	4.0	CVE-2017-7589 MISC (link is external) CONFIRM (link is external)
openidm_project -- openidm	OpenIDM through 4.0.0 and 4.5.0 is vulnerable to persistent cross-site scripting (XSS) attacks within the Admin UI, as demonstrated by a crafted Managed Object Name.	2017-04-08	4.3	CVE-2017-7590 MISC (link is external) CONFIRM (link is external)
openidm_project -- openidm	OpenIDM through 4.0.0 and 4.5.0 is vulnerable to reflected cross-site scripting (XSS) attacks within the Admin UI, as demonstrated by the _sortKeys parameter to the authzRoles script under managed/user/.	2017-04-08	4.3	CVE-2017-7591 MISC (link is external) CONFIRM (link is external)
opmantek -- network_management_information_system	Opmantek NMIS before 4.3.7c has command injection via man, finger, ping, trace, and nslookup in the tools.pl CGI script. Versions before 8.5.12G might be affected in non-default configurations.	2017-04-09	6.0	CVE-2016-6534 MISC (link is external)
opsview -- opsview	Opsview before 2015-11-06 has XSS via SNMP.	2017-04-09	4.3	CVE-2015-6035 MISC (link is external)

osram -- lightify_home	OSRAM SYLVANIA Osram Lightify Home before 2016-07-26 stores a PSK in cleartext under /private/var/mobile/Containers/Data/Application.	2017-04-09	5.0	CVE-2016-5051 MISC (link is external)
osram -- lightify_home	OSRAM SYLVANIA Osram Lightify Home through 2016-07-26 does not use SSL pinning.	2017-04-09	5.0	CVE-2016-5052 MISC (link is external)
osram -- lightify_home	OSRAM SYLVANIA Osram Lightify Home through 2016-07-26 allows Zigbee replay.	2017-04-09	5.0	CVE-2016-5054 MISC (link is external)
osram -- lightify_pro	OSRAM SYLVANIA Osram Lightify Pro before 2016-07-26 has XSS in the username field and Wireless Client Mode configuration page.	2017-04-09	4.3	CVE-2016-5055 MISC (link is external)
osram -- lightify_pro	OSRAM SYLVANIA Osram Lightify Pro before 2016-07-26 uses only 8 hex digits for a PSK.	2017-04-09	5.0	CVE-2016-5056 MISC (link is external)
osram -- lightify_pro	OSRAM SYLVANIA Osram Lightify Pro through 2016-07-26 does not use SSL pinning.	2017-04-09	5.0	CVE-2016-5057 MISC (link is external)
osram -- lightify_pro	OSRAM SYLVANIA Osram Lightify Pro through 2016-07-26 allows Zigbee replay.	2017-04-09	5.0	CVE-2016-5058 MISC (link is external)
osram -- lightify_pro	OSRAM SYLVANIA Osram Lightify Pro before 2016-07-26 allows attackers to obtain sensitive information by reading screenshots under /private/var/mobile/Containers/Data/Application.	2017-04-09	4.0	CVE-2016-5059 MISC (link is external)
oxidforge -- oxid_eshop	OXID eShop before 2016-06-13 allows remote attackers to execute arbitrary code via a GET or POST request to the oxuser class. Fixed versions are Enterprise Edition v5.1.12, Enterprise Edition v5.2.9, Professional Edition v4.8.12, Professional Edition v4.9.9, Community Edition v4.8.12, Community Edition v4.9.9.	2017-04-09	6.5	CVE-2016-5072 MISC
paessler -- prtg	Paessler PRTG before 16.2.24.4045 has XSS via SNMP.	2017-04-09	4.3	CVE-2016-5078 MISC (link is external)
philips -- in.sight_b120\37	Philips In.Sight B120/37 allows remote attackers to obtain sensitive information via a direct request, related to yoics.net URLs, stream.m3u8 URIs, and cam_service_enable.cgi.	2017-04-09	5.0	CVE-2015-2884 MISC (link is external)
phpmyfaq -- phpmyfaq	inc/PMF/Faq.php in phpMyFAQ before 2.9.7 has XSS in the question field.	2017-04-07	4.3	CVE-2017-7579 CONFIRM (link

				is external) CONFIRM (link is external)
pivotx -- pivotx	PivotX 2.3.11 allows remote authenticated Advanced users to execute arbitrary PHP code by performing an upload with a safe file extension (such as .jpg) and then invoking the duplicate function to change to the .php extension.	2017-04-07	6.5	CVE-2017-7570 MISC (link is external)
proxygen_project -- proxygen	The SPDY/2 codec in Facebook Proxygen before 2015-11-09 allows remote attackers to conduct hijacking attacks and bypass ACL checks via a crafted host value.	2017-04-09	5.0	CVE-2015-7263 MISC (link is external)
proxygen_project -- proxygen	Facebook Proxygen before 2015-11-09 mismanages HTTPMessage.request state, which allows remote attackers to conduct hijacking attacks and bypass ACL checks.	2017-04-09	5.0	CVE-2015-7265 MISC (link is external)
sap -- netweaver	The SAP EP-RUNTIME component in SAP NetWeaver AS JAVA 7.5 allows remote authenticated users to cause a denial of service (out-of-memory error and service instability) via a crafted serialized Java object, as demonstrated by serial.cc3, aka SAP Security Note 2315788.	2017-04-10	4.0	CVE-2016-10304 MISC (link is external)
sap -- sql_anywhere	Buffer overflow in the MobiLink Synchronization Server component in SAP SQL Anywhere 17 and possibly earlier allows remote authenticated users to cause a denial of service (resource consumption and process crash) by sending a crafted packet several times, aka SAP Security Note 2308778.	2017-04-10	4.0	CVE-2016-10310 BID (link is external) MISC (link is external)
schneider-electric -- interactive_graphical_scada_system	A DLL Hijacking issue was discovered in Schneider Electric Interactive Graphical SCADA System (IGSS) Software, Version 12 and previous versions. The software will execute a malicious file if it is named the same as a legitimate file and placed in a location that is earlier in the search path.	2017-04-07	6.8	CVE-2017-6033 CONFIRM (link is external) BID (link is external) MISC
sierrawireless -- aleos_firmware	Sierra Wireless GX 440 devices with ALEOS firmware 4.3.2 store passwords in cleartext.	2017-04-09	5.0	CVE-2016-5070 MISC (link is external)
spiceworks -- desktop	Spiceworks Desktop before 2015-12-01 has XSS via an SNMP response.	2017-04-09	4.3	CVE-2015-6021 MISC (link is

				external)
summer_infant -- baby_zoom_wifi_monitor_firmware	Summer Baby Zoom Wifi Monitor & Internet Viewing System allows remote attackers to gain privileges via manual entry of a Settings URL.	2017-04-09	6.5	CVE-2015-2889 MISC (link is external)
swagger_project -- swagger-ui	Swagger-UI before 2.2.1 has XSS via the Default field in the Definitions section.	2017-04-09	4.3	CVE-2016-5682 MISC (link is external)
visioncritical -- vision_critical	Vision Critical before 2014-05-30 allows attackers to read arbitrary files via unspecified vectors, as demonstrated by image files and configuration files.	2017-04-09	5.0	CVE-2014-2960 MISC (link is external)
web2py -- web2py	web2py before 2.14.6 does not properly check if a host is denied before verifying passwords, allowing a remote attacker to perform brute-force attacks.	2017-04-10	5.0	CVE-2016-10321 CONFIRM (link is external) CONFIRM (link is external)
xiongmai_technologies -- uc-httpd	XiongMai uc-httpd has directory traversal allowing the reading of arbitrary files via a "GET ../" HTTP request.	2017-04-07	5.0	CVE-2017-7577 MISC (link is external)

Low Severity Vulnerabilities

The Primary Vendor --- Product	Description	Date Published	CVSS Score	The CVE Identity
apple -- apple_music	The Apple Music (aka com.apple.android.music) application before 2.0 for Android does not 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.	2017-04-07	2.9	CVE-2017-2387 MISC (link is external) BID (link is external) CONFIRM (link is external)
atlassian -- confluence	Atlassian Confluence Server before 5.9.11 has XSS on the viewmyprofile.action page.	2017-04-09	3.5	CVE-2016-4317 BID (link is external) MISC (link is

				external)
atlassian -- jira	Atlassian JIRA Server before 7.1.9 has XSS in project/ViewDefaultProjectRoleActors.jspa via a role name.	2017-04-09	3.5	CVE-2016-4318 BID (link is external) MISC (link is external)
cisco -- firepower_extensible_operating_system	A vulnerability in the CLI of the Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to perform a command injection attack. More Information: CSCvb61384 CSCvb86764. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.101) 92.1(1.1647).	2017-04-07	3.6	CVE-2017-6601 BID (link is external) CONFIRM (link is external)
cisco -- firepower_extensible_operating_system	A vulnerability in the CLI of Cisco Unified Computing System (UCS) Manager, Cisco Firepower 4100 Series Next-Generation Firewall (NGFW), and Cisco Firepower 9300 Security Appliance could allow an authenticated, local attacker to perform a command injection attack. More Information: CSCvb66189 CSCvb86775. Known Affected Releases: 2.0(1.68) 3.1(1k)A. Known Fixed Releases: 92.2(1.101) 92.1(1.1742) 92.1(1.1658) 2.1(1.38) 2.0(1.107) 2.0(1.87) 1.1(4.148) 1.1(4.138).	2017-04-07	3.6	CVE-2017-6602 BID (link is external) CONFIRM (link is external)
cisco -- unified_communications_manager	A vulnerability in the web-based management interface of Cisco Unified Communications Manager could allow an authenticated, remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management interface of an affected device. This vulnerability affects Cisco Unified Communications Manager with a default configuration running an affected software release with the attacker authenticated as the administrative user. More Information: CSCvc83712. Known Affected Releases: 12.0(0.98000.452). Known Fixed Releases: 12.0(0.98000.750) 12.0(0.98000.708) 12.0(0.98000.707) 12.0(0.98000.704) 12.0(0.98000.554) 12.0(0.98000.546) 12.0(0.98000.543) 12.0(0.98000.248)	2017-04-07	3.5	CVE-2017-3888 BID (link is external) CONFIRM (link is external)

	12.0(0.98000.244) 12.0(0.98000.242).			
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm Wi-Fi driver 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-32074353. References: QC-CR#1104731.	2017-04-07	2.6	CVE-2017-0584 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An information disclosure vulnerability in the Broadcom Wi-Fi driver 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-32475556. References: B-RB#112953.	2017-04-07	2.6	CVE-2017-0585 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm sound driver 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-33649808. References: QC-CR#1097569.	2017-04-07	2.6	CVE-2017-0586 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	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.	2017-04-10	2.1	CVE-2017-7616 CONFIRM BID (link is external) CONFIRM (link is external)
opmantek -- network_management_information_system	Opmantek NMIS before 8.5.12G has XSS via SNMP.	2017-04-09	3.5	CVE-2016-5642 MISC (link is external)
philips -- in.sight_b120\37	Philips In.Sight B120/37 has XSS, related to the Weaved cloud web service, as demonstrated by the name parameter to deviceSettings.php or shareDevice.php.	2017-04-09	3.5	CVE-2015-2883 MISC (link is external)

- Sources: http://nvd.nist.gov (For more information visit the National Vulnerabilities Database (NVD) which contains a database of every vulnerability that has ever been published).

Uganda Communications Commission – UGCERT
Email: info@ug-cert.ug Tel + 256 414 302 100/150 **Toll Free:** 0800 133 911
Website www.ug-cert.ug Face book / Twitter: UGCERT