Vulnerability Summary for the Week of March 6, 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**
admidio -- admidio	SQL Injection was discovered in adm_program/modules/dates/dates_function.php in Admidio 3.2.5. The POST parameter dat_cat_id is concatenated into a SQL query without any input validation/sanitization.	2017-03-05	9.0	CVE-2017-6492 MISC (link is external)
apache -- camel	Apache Camel's camel-jackson and camel-jacksonxml components are vulnerable to Java object de-serialization vulnerability. Camel allows to specify such a type through the 'CamelJacksonUnmarshalType' property. De-serializing untrusted data can lead to security flaws as demonstrated in various similar reports about Java de-serialization issues.	2017-03-07	7.5	CVE-2016-9571 CONFIRM BID (link is external)
apache -- camel	Apache Camel's camel-snakeyaml component is vulnerable to Java object de-serialization vulnerability. De-serializing untrusted data can lead to security flaws.	2017-03-07	7.5	CVE-2017-3159 CONFIRM
asus -- rt-ac53_firmware	Buffer overflows in networkmap in ASUS ASUSWRT on RT-AC53 3.0.0.4.380.6038 devices	2017-03-09	10.0	CVE-2017-6548 MISC (link is external)

	allow remote attackers to execute arbitrary code on the router via a long host or port in crafted multicast messages.			
asus -- rt-ac53_firmware	Session hijack vulnerability in httpd in ASUS ASUSWRT on RT-AC53 3.0.0.4.380.6038 devices allows remote attackers to steal any active admin session by sending cgi_logout and asusrouter-Windows-IFTTT-1.0 in certain HTTP headers.	2017-03-09	9.3	CVE-2017-6549 MISC (link is external)
d-link -- di-524_firmware	Multiple cross-site request forgery (CSRF) vulnerabilities on the D-Link DI-524 Wireless Router with firmware 9.01 allow remote attackers to (1) change the admin password, (2) reboot the device, or (3) possibly have unspecified other impact via crafted requests to CGI programs.	2017-03-06	8.5	CVE-2017-5633 MISC BID (link is external)
debian -- debian_linux	Heap-based buffer overflow in the create_url_list function in gena/gena_device.c in Portable UPnP SDK (aka libupnp) before 1.6.21 allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a valid URI followed by an invalid one in the CALLBACK header of an SUBSCRIBE request.	2017-03-07	7.5	CVE-2016-8863 BID (link is external) CONFIRM (link is external) CONFIRM (link is external) DEBIAN
espeak-ruby_project -- espeak-ruby	The espeak-ruby gem before 1.0.3 for Ruby allows remote attackers to execute arbitrary commands via shell metacharacters in a string to the speak, save, bytes or bytes_wav method in lib/espeak/speech.rb.	2017-03-03	7.5	CVE-2016-10193 MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
exponentcms -- exponent_cms	SQL injection vulnerability in cron/find_help.php in Exponent CMS 2.3.9 and earlier allows remote attackers to execute arbitrary SQL commands via the version parameter.	2017-03-07	7.5	CVE-2016-7780 MISC (link is external) FULLDISC CONFIRM (link is external)
exponentcms -- exponent_cms	SQL injection vulnerability in framework/modules/blog/controllers/blogController.php in Exponent CMS 2.3.9 and earlier allows remote attackers to execute arbitrary SQL	2017-03-07	7.5	CVE-2016-7781 MISC (link is external) FULLDISC CONFIRM (link is external)

	commands via the author parameter.			
exponentcms -- exponent_cms	SQL injection vulnerability in framework/core/models/expConfig.php in Exponent CMS 2.3.9 and earlier allows remote attackers to execute arbitrary SQL commands via the src parameter.	2017-03-07	7.5	CVE-2016-7782 MISC (link is external) FULLDISC
exponentcms -- exponent_cms	SQL injection vulnerability in framework/core/models/expRecord.php in Exponent CMS 2.3.9 and earlier allows remote attackers to execute arbitrary SQL commands via the title parameter.	2017-03-07	7.5	CVE-2016-7783 MISC (link is external) FULLDISC
exponentcms -- exponent_cms	SQL injection vulnerability in the getSection function in framework/core/subsystems/expRouter.php in Exponent CMS 2.3.9 and earlier allows remote attackers to execute arbitrary SQL commands via the section parameter.	2017-03-07	7.5	CVE-2016-7784 MISC (link is external) FULLDISC CONFIRM (link is external)
exponentcms -- exponent_cms	SQL injection vulnerability in ramework/modules/users/models/user.php in Exponent CMS 2.3.9 and earlier allows remote attackers to execute arbitrary SQL commands via the username parameter.	2017-03-07	7.5	CVE-2016-7788 MISC (link is external) FULLDISC CONFIRM (link is external)
exponentcms -- exponent_cms	SQL injection vulnerability in framework/core/models/expConfig.php in Exponent CMS 2.3.9 and earlier allows remote attackers to execute arbitrary SQL commands via the apikey parameter.	2017-03-07	7.5	CVE-2016-7789 MISC MISC (link is external) FULLDISC
exponentcms -- exponent_cms	SQL injection vulnerability in the activate_address function in framework/modules/addressbook/controllers/addressController.php in Exponent CMS 2.3.9 and earlier allows remote attackers to execute arbitrary SQL commands via the is_what parameter.	2017-03-07	7.5	CVE-2016-9019 MISC MISC (link is external) FULLDISC
exponentcms -- exponent_cms	SQL injection vulnerability in framework/modules/help/controllers/helpController.php in Exponent CMS 2.3.9 and earlier allows remote attackers to execute arbitrary SQL	2017-03-07	7.5	CVE-2016-9020 MISC (link is external) FULLDISC CONFIRM (link

	commands via the version parameter.			is external)
exponentcms -- exponent_cms	SQL injection vulnerability in framework/modules/filedownloads/controllers/filedownloadController.php in Exponent CMS 2.3.9 and earlier allows remote attackers to execute arbitrary SQL commands via the fileid parameter.	2017-03-07	7.5	CVE-2016-9087 MISC (link is external) FULLDISC CONFIRM (link is external)
festivaltts4r_project -- festivaltts4r	The festivaltts4r gem for Ruby allows remote attackers to execute arbitrary commands via shell metacharacters in a string to the (1) to_speech or (2) to_mp3 method in lib/festivaltts4r/festival4r.rb.	2017-03-03	7.5	CVE-2016-10194 MLIST (link is external) MLIST (link is external) MISC (link is external)
flexense -- sysgauge	An issue was discovered in SysGauge 1.5.18. A buffer overflow vulnerability in SMTP connection verification leads to arbitrary code execution. The attack vector is a crafted SMTP daemon that sends a long 220 (aka "Service ready") string.	2017-03-05	7.5	CVE-2017-6416 BID (link is external) EXPLOIT-DB (link is external)
google -- android	A remote code execution vulnerability 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-33139050.	2017-03-07	9.3	CVE-2017-0466 BID (link is external) MISC (link is external)
google -- android	A remote code execution vulnerability 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-33250932.	2017-03-07	9.3	CVE-2017-0467 BID (link is external) MISC (link is external)
google -- android	A remote code execution vulnerability in Mediaserver could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue	2017-03-07	9.3	CVE-2017-0468 BID (link is external) MISC (link is external)

	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-33351708.			
google -- android	A remote code execution vulnerability 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-33450635.	2017-03-07	9.3	CVE-2017-0469 BID (link is external) MISC (link is external)
google -- android	A remote code execution vulnerability 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-33818500.	2017-03-07	9.3	CVE-2017-0470 BID (link is external) MISC (link is external)
google -- android	A remote code execution vulnerability 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-33816782.	2017-03-07	9.3	CVE-2017-0471 BID (link is external) MISC (link is external)
google -- android	A remote code execution vulnerability 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-33862021.	2017-03-07	9.3	CVE-2017-0472 BID (link is external) MISC (link is external)
google -- android	A remote code execution vulnerability in Mediaserver could enable an attacker using a	2017-03-07	9.3	CVE-2017-0473 BID (link is external)

	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-33982658.			MISC (link is external)
google -- android	A remote code execution vulnerability 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: 7.0, 7.1.1. Android ID: A-32589224.	2017-03-07	9.3	CVE-2017-0474 BID (link is external) MISC (link is external)
google -- android	An elevation of privilege vulnerability in the recovery verifier 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: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-31914369.	2017-03-07	9.3	CVE-2017-0475 BID (link is external) MISC (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: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32707507.	2017-03-07	9.3	CVE-2017-0479 MISC (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	2017-03-07	9.3	CVE-2017-0480 MISC (link is external)

	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-32705429.			
google -- android	An elevation of privilege vulnerability in NFC could enable a proximate attacker 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-33434992.	2017-03-07	9.3	CVE-2017-0481 MISC (link is external)
google -- android	A denial of service vulnerability 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-33090864.	2017-03-07	7.1	CVE-2017-0482 MISC (link is external)
google -- android	A denial of service vulnerability 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: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33137046.	2017-03-07	7.1	CVE-2017-0483 MISC (link is external)
google -- android	A denial of service vulnerability 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-33298089.	2017-03-07	7.1	CVE-2017-0484 MISC (link is external)
google -- android	A denial of service vulnerability in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This	2017-03-07	7.1	CVE-2017-0485 MISC (link is external)

	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-33387820.			
google -- android	A denial of service vulnerability 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-33621215.	2017-03-07	7.1	CVE-2017-0486 MISC (link is external)
google -- android	A denial of service vulnerability 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-33751193.	2017-03-07	7.1	CVE-2017-0487 MISC (link is external)
google -- android	A denial of service vulnerability 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-34097213.	2017-03-07	7.1	CVE-2017-0488 MISC (link is external)
google -- android	A denial of service vulnerability in Audioserver could enable a local malicious application to cause a device hang or reboot. This issue is rated as Low due to the possibility of a temporary denial of service. Product: Android. Versions: 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32095713.	2017-03-07	7.1	CVE-2017-0499 MISC (link is external)
google -- android	An elevation of privilege vulnerability in MediaTek components, including the M4U driver, sound driver, touchscreen driver, GPU driver, and Command Queue driver, could enable a local malicious application to execute arbitrary code within the context of the kernel.	2017-03-07	9.3	CVE-2017-0500 BID (link is external) MISC (link is external)

	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-28429685. References: M-ALPS02710006.			
google -- android	An elevation of privilege vulnerability in MediaTek components, including the M4U driver, sound driver, touchscreen driver, GPU driver, and Command Queue 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-28430015. References: M-ALPS02708983.	2017-03-07	9.3	CVE-2017-0501 BID (link is external) MISC (link is external)
google -- android	An elevation of privilege vulnerability in MediaTek components, including the M4U driver, sound driver, touchscreen driver, GPU driver, and Command Queue 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-28430164. References: M-ALPS02710027.	2017-03-07	9.3	CVE-2017-0502 BID (link is external) MISC (link is external)
google -- android	An elevation of privilege vulnerability in MediaTek components, including the M4U driver, sound driver, touchscreen driver, GPU driver, and Command Queue 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	2017-03-07	9.3	CVE-2017-0503 BID (link is external) MISC (link is external)

	operating system to repair the device. Product: Android. Versions: N/A. Android ID: A-28449045. References: M-ALPS02710075.			
google -- android	An elevation of privilege vulnerability in MediaTek components, including the M4U driver, sound driver, touchscreen driver, GPU driver, and Command Queue 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-30074628. References: M-ALPS02829371.	2017-03-07	9.3	CVE-2017-0504 BID (link is external) MISC (link is external)
google -- android	An elevation of privilege vulnerability in MediaTek components, including the M4U driver, sound driver, touchscreen driver, GPU driver, and Command Queue 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-31822282. References: M-ALPS02992041.	2017-03-07	9.3	CVE-2017-0505 BID (link is external) MISC (link is external)
google -- android	An elevation of privilege vulnerability in MediaTek components, including the M4U driver, sound driver, touchscreen driver, GPU driver, and Command Queue 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-32276718. References: M-ALPS03006904.	2017-03-07	9.3	CVE-2017-0506 BID (link is external) MISC (link is external)

google -- android	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 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-32124445. References: B-RB#110688.	2017-03-07	9.3	CVE-2017-0509 MISC (link is external)
google -- android	An elevation of privilege vulnerability in the MediaTek hardware sensor 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-32372051. References: M-ALPS02973195.	2017-03-07	7.6	CVE-2017-0517 MISC (link is external)
google -- android	An elevation of privilege vulnerability in a MediaTek APK could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High due to the possibility of local arbitrary code execution in a privileged process. Product: Android. Versions: N/A. Android ID: A-32916158. References: M-ALPS03032516.	2017-03-07	9.3	CVE-2017-0522 MISC (link is external)
google -- android	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: N/A. Android ID: A-32835279. References: QC-CR#1096945.	2017-03-07	7.6	CVE-2017-0523 MISC (link is external) CONFIRM
ibm -- qradar_security_information_and_event_manager	IBM QRadar 7.2 is vulnerable to a denial of service, caused by an XML External Entity Injection (XXE) error when processing XML data. A remote attacker could exploit this vulnerability to expose highly sensitive information or	2017-03-07	7.5	CVE-2016-9724 CONFIRM (link is external)

	consume all available memory resources. IBM Reference #: 1999537.			
ibm -- qradar_security_information_and_event_manager	IBM QRadar Incident Forensics 7.2 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM Reference #: 1999542.	2017-03-07	9.0	CVE-2016-9726 CONFIRM (link is external)
ibm -- qradar_security_information_and_event_manager	IBM QRadar 7.2 could allow a remote authenticated attacker to execute arbitrary commands on the system. By sending a specially-crafted request, an attacker could exploit this vulnerability to execute arbitrary commands on the system. IBM Reference #: 1999542.	2017-03-07	8.5	CVE-2016-9727 CONFIRM (link is external)
ibm -- qradar_security_information_and_event_manager	IBM QRadar 7.2 could allow a remote attacker to consume all resources on the server due to not properly restricting the size or amount of resources requested by an actor. IBM Reference #: 1999556.	2017-03-07	7.8	CVE-2016-9740 CONFIRM (link is external) BID (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm camera 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 is mitigated by current platform configurations. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32342399. References: QC-CR#1088824.	2017-03-07	7.6	CVE-2016-8417 MISC (link is external) CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm GPU 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	2017-03-07	9.3	CVE-2016-8479 MISC (link is external)

	the device. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31824853. References: QC-CR#1093687.			
linux -- linux_kernel	An elevation of privilege vulnerability in the NVIDIA GPU 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-34132950. References: N-CVE-2017-0306.	2017-03-07	9.3	CVE-2017-0306 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the NVIDIA GPU 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-3.18. Android ID: A-33177895. References: N-CVE-2017-0307.	2017-03-07	9.3	CVE-2017-0307 CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the NVIDIA GPU 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-3.18. Android ID: A-33899363. References: N-CVE-2017-0333.	2017-03-07	9.3	CVE-2017-0333 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the NVIDIA GPU 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	2017-03-07	9.3	CVE-2017-0335 BID (link is external) CONFIRM (link is external)

	require reflashing the operating system to repair the device. Product: Android. Versions: Kernel-3.18. Android ID: A-33043375. References: N-CVE-2017-0335.			
linux -- linux_kernel	An elevation of privilege vulnerability in the NVIDIA GPU 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-3.18. Android ID: A-31992762. References: N-CVE-2017-0337.	2017-03-07	9.3	CVE-2017-0337 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the NVIDIA GPU 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-3.18. Android ID: A-33057977. References: N-CVE-2017-0338.	2017-03-07	9.3	CVE-2017-0338 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. Android ID: A-33979145. References: QC-CR#1105085.	2017-03-07	7.6	CVE-2017-0453 MISC (link is external) CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm bootloader could help to enable a local malicious application to to execute arbitrary code within the context of the bootloader. This issue is rated as High because it is a general bypass for a bootloader level defense in depth or exploit mitigation	2017-03-07	9.3	CVE-2017-0455 MISC (link is external) CONFIRM

	technology. Product: Android. Versions: Kernel-3.18. Android ID: A-32370952. References: QC-CR#1082755.			
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm IPA 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-33106520. References: QC-CR#1099598.	2017-03-07	7.6	CVE-2017-0456 MISC (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm ADSPRPC 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-31695439. References: QC-CR#1086123, QC-CR#1100695.	2017-03-07	7.6	CVE-2017-0457 MISC (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm 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: Kernel-3.18. Android ID: A-32588962. References: QC-CR#1089433.	2017-03-07	7.6	CVE-2017-0458 MISC (link is external) CONFIRM
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm networking 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-31252965. References: QC-CR#1098801.	2017-03-07	7.6	CVE-2017-0460 MISC (link is external)

linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm networking 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-33277611. References: QC-CR#1101792.	2017-03-07	7.6	CVE-2017-0463 MISC (link is external) CONFIRM
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-32940193. References: QC-CR#1102593.	2017-03-07	7.6	CVE-2017-0464 MISC (link is external) CONFIRM
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-31992382.	2017-03-07	9.3	CVE-2017-0507 MISC (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-3.18. Android ID: A-33940449.	2017-03-07	9.3	CVE-2017-0508 MISC (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the kernel FIQ debugger could enable a local malicious application to execute arbitrary code	2017-03-07	9.3	CVE-2017-0510 MISC (link is external)

	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-32402555.			
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm input hardware 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-32341680. References: QC-CR#1096301.	2017-03-07	7.6	CVE-2017-0516 MISC (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm fingerprint sensor 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-32370896. References: QC-CR#1086530.	2017-03-07	7.6	CVE-2017-0518 MISC (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm fingerprint sensor 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-32372915. References: QC-CR#1086530.	2017-03-07	7.6	CVE-2017-0519 MISC (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-31750232. References: QC-	2017-03-07	7.6	CVE-2017-0520 MISC (link is external) CONFIRM

	CR#1082636.			
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm 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: Kernel-3.10, Kernel-3.18. Android ID: A-32919951. References: QC-CR#1097709.	2017-03-07	7.6	CVE-2017-0521 MISC (link is external) CONFIRM
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-3.10, Kernel-3.18. Android ID: A-33002026.	2017-03-07	7.6	CVE-2017-0524 MISC (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm IPA 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-33139056. References: QC-CR#1097714.	2017-03-07	7.6	CVE-2017-0525 MISC (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the HTC Sensor Hub 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-33897738.	2017-03-07	7.6	CVE-2017-0526 MISC (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the HTC Sensor Hub Driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High	2017-03-07	7.6	CVE-2017-0527 MISC (link is external)

	because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-33899318.			
linux -- linux_kernel	An elevation of privilege vulnerability in the kernel security subsystem could enable a local malicious application to to execute code in the context of a privileged process. This issue is rated as High because it is a general bypass for a kernel level defense in depth or exploit mitigation technology. Product: Android. Versions: Kernel-3.18. Android ID: A-33351919.	2017-03-07	9.3	CVE-2017-0528 MISC (link is external)
linux -- linux_kernel	Race condition in drivers/tty/n_hdlc.c in the Linux kernel through 4.10.1 allows local users to gain privileges or cause a denial of service (double free) by setting the HDLC line discipline.	2017-03-07	7.2	CVE-2017-2636 MLIST (link is external) CONFIRM (link is external)
nefarious2_project -- nefarious2	The m_authenticate function in ircd/m_authenticate.c in nefarious2 allows remote attackers to spoof certificate fingerprints and consequently log in as another user via a crafted AUTHENTICATE parameter.	2017-03-07	7.5	CVE-2016-7145 MLIST (link is external) CONFIRM (link is external)
netgear -- dgn2200_series_firmware	dnslookup.cgi on NETGEAR DGN2200 devices with firmware through 10.0.0.50 allows remote authenticated users to execute arbitrary OS commands via shell metacharacters in the host_name field of an HTTP POST request, a different vulnerability than CVE-2017-6077.	2017-03-05	9.0	CVE-2017-6334 BID (link is external) EXPLOIT-DB (link is external)
openbsd -- openbsd	Integer truncation error in the amap_alloc function in OpenBSD 5.8 and 5.9 allows local users to execute arbitrary code with kernel privileges via a large size value.	2017-03-07	7.2	CVE-2016-6240 CONFIRM CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external)
openbsd -- openbsd	Integer overflow in the amap_alloc1 function in OpenBSD 5.8 and 5.9 allows local users to execute arbitrary code with kernel privileges via a large size value.	2017-03-07	7.2	CVE-2016-6241 CONFIRM CONFIRM MLIST (link is external)

				MLIST (link is external) BID (link is external)
openbsd -- openbsd	The sys_thrsigdivert function in kern/kern_sig.c in the OpenBSD kernel 5.9 allows remote attackers to cause a denial of service (panic) via a negative "ts.tv_sec" value.	2017-03-07	7.8	CVE-2016-6244 MLIST (link is external) BID (link is external)
openelec -- openelec	The auto-update feature of Open Embedded Linux Entertainment Center (OpenELEC) 6.0.3 and 7.0.1 uses neither encrypted connections nor signed updates. A man-in-the-middle attacker could manipulate the update packages to gain root access remotely.	2017-03-05	7.6	CVE-2017-6445 BID (link is external) MISC (link is external)
revive-adserver -- revive_adserver	Revive Adserver before 4.0.1 allows remote attackers to execute arbitrary code via serialized data in the cookies related to the delivery scripts.	2017-03-03	7.5	CVE-2017-5830 MLIST (link is external) BID (link is external) CONFIRM (link is external)
wireshark -- wireshark	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is an IAX2 infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-iax2.c by constraining packet lateness.	2017-03-03	7.8	CVE-2017-6470 CONFIRM CONFIRM CONFIRM
zoneminder -- zoneminder	SQL injection vulnerability in Zoneminder 1.30 and earlier allows remote attackers to execute arbitrary SQL commands via the limit parameter in a log query request to index.php.	2017-03-03	7.5	CVE-2016-10204 MLIST (link is external) MISC (link is external)
zoneminder -- zoneminder	Session fixation vulnerability in Zoneminder 1.30 and earlier allows remote attackers to hijack web sessions via the ZMSESSID cookie.	2017-03-03	7.5	CVE-2016-10205 MLIST (link is external) MISC (link is external)

Medium Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
agora-project -- agora-project	XSS in Agora-Project 3.2.2 exists with an index.php?disconnect=1&msgNotif[]=[XSS] attack.	2017-03-09	4.3	CVE-2017-6559 MISC (link is external)
agora-project -- agora-project	XSS in Agora-Project 3.2.2 exists with an index.php?ctrl=misc&action=[XSS]&editObjId=[XSS] attack.	2017-03-09	4.3	CVE-2017-6560 MISC (link is external)
agora-project -- agora-project	XSS in Agora-Project 3.2.2 exists with an index.php?ctrl=object&action=[XSS] attack.	2017-03-09	4.3	CVE-2017-6561 MISC (link is external)
agora-project -- agora-project	XSS in Agora-Project 3.2.2 exists with an index.php?ctrl=file&targetObjId=fileFolder-2&targetObjIdChild=[XSS] attack.	2017-03-09	4.3	CVE-2017-6562 MISC (link is external)
asus -- rt-ac53_firmware	Cross-site scripting (XSS) vulnerability in httpd in ASUS ASUSWRT on RT-AC53 3.0.0.4.380.6038 devices allows remote attackers to inject arbitrary JavaScript by requesting filenames longer than 50 characters.	2017-03-09	4.3	CVE-2017-6547 MISC (link is external)
atutor -- atutor	Multiple Cross-Site Scripting (XSS) issues were discovered in ATutor 2.2.2. The vulnerabilities exist due to insufficient filtration of user-supplied data passed to several pages (lang_code in themes/*/admin/system_preferences/language_edit.tmpl.php). An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-05	4.3	CVE-2017-6483 BID (link is external) CONFIRM (link is external)
blackberry -- good_control_server	An information disclosure vulnerability in the logging implementation of BlackBerry Good Control Server versions earlier than 2.3.53.62 allows remote attackers to gain and use logged encryption keys to access certain resources within a customer's Good deployment by gaining access to certain diagnostic log files through either a valid logon or an unrelated compromise of the server.	2017-03-03	5.0	CVE-2016-3127 CONFIRM (link is external) BID (link is external)

burgundy-cms_project -- burgundy-cms	Smith0r/burgundy-cms before 2017-03-06 is vulnerable to a reflected XSS in admin/components/menu/views/menuitems.php (id parameter).	2017-03-07	4.3	CVE-2017-6509 CONFIRM (link is external)
ca -- service_desk_manager	Cross-site scripting (XSS) vulnerability in CA Service Desk Manager (formerly CA Service Desk) 12.9 and 14.1 allows remote attackers to inject arbitrary web script or HTML via the QBE.EQ.REF_NUM parameter.	2017-03-07	4.3	CVE-2016-9148 MISC (link is external) FULLDISC CONFIRM (link is external) BID (link is external) SECTRACK (link is external)
ca -- unified_infrastructure_management	Directory traversal vulnerability in diag.jsp file in CA Unified Infrastructure Management (formerly CA Nimsoft Monitor) 8.4 SP1 and earlier and CA Unified Infrastructure Management Snap (formerly CA Nimsoft Monitor Snap) allows remote attackers to read arbitrary files via unspecified vectors.	2017-03-07	5.0	CVE-2016-9164 MISC (link is external) FULLDISC BID (link is external) MISC (link is external) CONFIRM (link is external)
cloudera -- hue	Multiple cross-site scripting (XSS) vulnerabilities in Cloudera HUE 3.9.0 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) First name or (2) Last name field in the HUE Users page.	2017-03-07	4.3	CVE-2016-4946 MISC (link is external) BID (link is external)
cloudera -- hue	Cloudera HUE 3.9.0 and earlier allows remote attackers to enumerate user accounts via a request to desktop/api/users/autocomplete.	2017-03-07	5.0	CVE-2016-4947 MISC (link is external) BID (link is external)
cloudera -- manager	Multiple cross-site scripting (XSS) vulnerabilities in Cloudera Manager 5.5 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) Template Name field when renaming a template; (2) KDC Server host, (3) Kerberos Security Realm, (4) Kerberos Encryption Types, (5) Advanced Configuration Snippet (Safety Valve) for [libdefaults] section of krb5.conf, (6) Advanced Configuration Snippet (Safety Valve) for the Default Realm in krb5.conf, (7) Advanced Configuration	2017-03-07	4.3	CVE-2016-4948 MISC (link is external) BID (link is external)

	Snippet (Safety Valve) for remaining krb5.conf, or (8) Active Directory Account Prefix fields in the Kerberos wizard; or (9) classicWizard parameter to cmf/cloudera-director/redirect.			
cloudera -- manager	Cloudera Manager 5.5 and earlier allows remote attackers to obtain sensitive information via a (1) stderr.log or (2) stdout.log value in the filename parameter to /cmf/process/<process_id>/logs.	2017-03-07	5.0	CVE-2016-4949 MISC (link is external) BID (link is external)
cloudera -- manager	Cloudera Manager 5.5 and earlier allows remote attackers to enumerate user sessions via a request to /api/v11/users/sessions.	2017-03-07	5.0	CVE-2016-4950 MISC (link is external) BID (link is external)
cpanel -- cgiemail	Format string vulnerability in cgiemail and cgiecho allows remote attackers to execute arbitrary code via format string specifiers in a template file.	2017-03-03	6.8	CVE-2017-5613 MLIST (link is external) BID (link is external) MISC (link is external)
cpanel -- cgiemail	Open redirect vulnerability in cgiemail and cgiecho allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via vectors involving the (1) success or (2) failure parameter.	2017-03-03	5.8	CVE-2017-5614 MLIST (link is external) BID (link is external) MISC (link is external)
cpanel -- cgiemail	cgiemail and cgiecho allow remote attackers to inject HTTP headers via a newline character in the redirect location.	2017-03-03	5.8	CVE-2017-5615 MLIST (link is external) BID (link is external) MISC (link is external)
cpanel -- cgiemail	Cross-site scripting (XSS) vulnerability in cgiemail and cgiecho allows remote attackers to inject arbitrary web script or HTML via the addendum parameter.	2017-03-03	4.3	CVE-2017-5616 MLIST (link is external) BID (link is external) MISC (link is external)
debian -- debian_linux	The getenv and filenameforall functions in Ghostscript 9.10 ignore the "-dSAFER" argument, which allows remote attackers to read data via a crafted postscript file.	2017-03-07	4.3	CVE-2013-5653 DEBIAN MLIST (link is external) MLIST (link is external)

				BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
debian -- debian_linux	The setByteArray function in tif_dir.c in libtiff 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted tiff image.	2017-03-07	4.3	CVE-2016-5315 DEBIAN MLIST (link is external) BID (link is external) CONFIRM (link is external) GENTOO
debian -- debian_linux	Portable UPnP SDK (aka libupnp) before 1.6.21 allows remote attackers to write to arbitrary files in the webroot via a POST request without a registered handler.	2017-03-07	5.0	CVE-2016-6255 DEBIAN MLIST (link is external) MLIST (link is external) BID (link is external) MISC (link is external) CONFIRM (link is external) MISC (link is external)
django-epiceditor_project -- django-epiceditor	There is a cross-site scripting vulnerability in django-epiceditor 0.2.3 via crafted content in a form field.	2017-03-09	4.3	CVE-2017-6591 MISC (link is external)
dlink -- dsl-2730u_firmware	Cross Site Request Forgery (CSRF) on D-Link DSL-2730U C1 IN_1.00 devices allows remote attackers to change the DNS or firewall configuration or any password.	2017-03-06	6.8	CVE-2017-6411 BID (link is external) EXPLOIT-DB (link is external)
dotclear -- dotclear	XSS was discovered in Dotclear v2.11.2, affecting admin/blogs.php and admin/users.php with the sortby and order parameters.	2017-03-05	4.3	CVE-2017-6446 BID (link is external) CONFIRM
epiceditor_project -- epiceditor	EpicEditor through 0.2.3 has Cross-Site Scripting because of an insecure default marked.js configuration. An example attack vector is a crafted IMG element in an HTML document.	2017-03-09	4.3	CVE-2017-6589 MISC (link is external)

fenix_hosting -- fenix-open-source	FenixHosting/fenix-open-source before 2017-03-04 is vulnerable to a reflected XSS in forums/search.php (search-by-topic parameter).	2017-03-05	4.3	CVE-2017-6479 BID (link is external) CONFIRM (link is external)
finecms_project -- finecms	andrzuk/FineCMS before 2017-03-06 is vulnerable to a reflected XSS in index.php because of missing validation of the action parameter in application/classes/application.php.	2017-03-07	4.3	CVE-2017-6511 CONFIRM (link is external) CONFIRM (link is external)
flexerasoftware -- flexnet_publisher	Open redirect vulnerability in the lmadmin component in Flexera FlexNet Publisher (aka Flex License Manager) 11.14.1 and earlier, as used in Citrix License Server for Windows and the Citrix License Server VPX, allows remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via unspecified vectors.	2017-03-03	5.8	CVE-2017-5571 BID (link is external) CONFIRM (link is external)
freetype -- freetype	The parse_charstrings function in type1/t1load.c in FreeType 2 before 2.7 does not ensure that a font contains a glyph name, which allows remote attackers to cause a denial of service (heap-based buffer over-read) or possibly have unspecified other impact via a crafted file.	2017-03-06	6.8	CVE-2016-10244 CONFIRM CONFIRM
gnu -- wget	CRLF injection vulnerability in the url_parse function in url.c in Wget through 1.19.1 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in the host subcomponent of a URL.	2017-03-07	4.3	CVE-2017-6508 CONFIRM MISC
google -- android	Race condition in the L2TPv3 IP Encapsulation feature in the Linux kernel before 4.8.14 allows local users to gain privileges or cause a denial of service (use-after-free) by making multiple bind system calls without properly ascertaining whether a socket has the SOCK_ZAPPED status, related to net/l2tp/l2tp_ip.c and net/l2tp/l2tp_ip6.c.	2017-03-07	6.9	CVE-2016-10200 CONFIRM CONFIRM (link is external) CONFIRM CONFIRM (link is external)
google -- android	A remote code execution vulnerability in AOSP Messaging could enable an attacker using a specially crafted file to cause memory corruption during media file and data processing. This issue is rated as High due to the possibility of remote code	2017-03-07	6.8	CVE-2017-0476 MISC (link is external)

	execution within the context of an unprivileged process. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33388925.			
google -- android	A remote code execution vulnerability in libgdx could enable an attacker using a specially crafted file to execute arbitrary code within the context of an unprivileged process. This issue is rated as High due to the possibility of remote code execution in an application that uses this library. Product: Android. Versions: 7.1.1. Android ID: A-33621647.	2017-03-07	6.8	CVE-2017-0477 MISC (link is external)
google -- android	A remote code execution vulnerability in the Framesequence library could enable an attacker using a specially crafted file to execute arbitrary code in the context of an unprivileged process. This issue is rated as High due to the possibility of remote code execution in an application that uses the Framesequence library. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33718716.	2017-03-07	6.8	CVE-2017-0478 MISC (link is external)
google -- android	An elevation of privilege vulnerability in Location Manager could enable a local malicious application to bypass operating system protections for location data. This issue is rated as Moderate because it could be used to generate inaccurate data. 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-33091107.	2017-03-07	4.3	CVE-2017-0489 MISC (link is external)
google -- android	An elevation of privilege vulnerability in Wi-Fi could enable a local malicious application to delete user data. This issue is rated as Moderate because it is a local bypass of user interaction requirements that would normally require either user initiation or user permission. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33178389.	2017-03-07	4.3	CVE-2017-0490 CONFIRM (link is external) MISC (link is external)
google -- android	An elevation of privilege vulnerability in Package Manager could enable a local malicious application to prevent users from uninstalling applications or removing permissions from applications. This issue is rated as Moderate because it is a local bypass of	2017-03-07	4.3	CVE-2017-0491 CONFIRM (link is external) MISC (link is external)

	user interaction requirements. 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-32553261.			
google -- android	An elevation of privilege vulnerability in the System UI could enable a local malicious application to create a UI overlay covering the entire screen. This issue is rated as Moderate because it is a local bypass of user interaction requirements that would normally require either user initiation or user permission. Product: Android. Versions: 7.1.1. Android ID: A-30150688.	2017-03-07	4.3	CVE-2017-0492 MISC (link is external)
google -- android	An information disclosure vulnerability in AOSP Messaging could enable a remote attacker using a special crafted file to access data outside of its permission levels. This issue is rated as Moderate because it could be used to access sensitive data without permission. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32764144.	2017-03-07	4.3	CVE-2017-0494 MISC (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 sensitive data without permission. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-33552073.	2017-03-07	4.3	CVE-2017-0495 MISC (link is external)
google -- android	A denial of service vulnerability in Setup Wizard could allow a local malicious application to temporarily block access to an affected device. This issue is rated as Moderate because it may require a factory reset to repair the device. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1. Android ID: A-31554152.	2017-03-07	4.3	CVE-2017-0496 MISC (link is external)
google -- android	A denial of service vulnerability in Mediaserver could enable an attacker to use a specially crafted file to cause a device hang or reboot. This issue is rated as Moderate because it requires an uncommon device configuration. Product: Android. Versions: 7.0, 7.1.1. Android ID: A-33300701.	2017-03-07	5.4	CVE-2017-0497 MISC (link is external)

google -- android	An information disclosure vulnerability in the MediaTek driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as High because it could be used to access sensitive data without explicit user permission. Product: Android. Versions: N/A. Android ID: A-28449427. References: M-ALPS02710042.	2017-03-07	4.3	CVE-2017-0529 MISC (link is external)
groovel_project -- cmsgroovel	groovel/cmsgroovel before 3.3.7-beta is vulnerable to a reflected XSS in commons/browser.php (path parameter).	2017-03-05	4.3	CVE-2017-6480 BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
ibm -- business_process_manager	IBM Business Process Manager 7.5, 8.0, and 8.5 has a file download capability that is vulnerable to a set of attacks. Ultimately, an attacker can cause an unauthenticated victim to download a malicious payload. An existing file type restriction can be bypassed so that the payload might be considered executable and cause damage on the victim's machine. IBM Reference #: 1998655.	2017-03-07	6.8	CVE-2016-9693 CONFIRM (link is external)
ibm -- qradar_security_information_and_event_manager	IBM QRadar 7.2 discloses sensitive information to unauthorized users. The information can be used to mount further attacks on the system. IBM Reference #: 1999533.	2017-03-07	5.0	CVE-2016-9720 CONFIRM (link is external) BID (link is external)
ibm -- qradar_security_information_and_event_manager	IBM QRadar 7.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 1999534.	2017-03-07	4.3	CVE-2016-9723 CONFIRM (link is external)
ibm -- qradar_security_information_and_event_manager	IBM QRadar Incident Forensics 7.2 allows for Cross-Origin Resource Sharing (CORS), which is a mechanism that allows web sites to request resources from external sites, avoiding the need to duplicate them. IBM Reference #: 1999539.	2017-03-07	5.0	CVE-2016-9725 CONFIRM (link is external) BID (link is external)
ibm -- qradar_security_inf	IBM Qradar 7.2 is vulnerable to SQL injection. A remote attacker could send specially-crafted SQL	2017-03-07	5.0	CVE-2016-9728 CONFIRM (link

ormation_and_event_manager	statements, which could allow the attacker to view, information in the back-end database. IBM Reference #: 1999543.			is external)
ibm -- qradar_security_information_and_event_manager	IBM QRadar 7.2 does not perform an authentication check for a critical resource or functionality allowing anonymous users access to protected areas. IBM Reference #: 1999545.	2017-03-07	6.4	CVE-2016-9729 CONFIRM (link is external) BID (link is external)
ibm -- qradar_security_information_and_event_manager	IBM QRadar Incident Forensics 7.2 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM Reference #: 1999549.	2017-03-07	4.3	CVE-2016-9730 CONFIRM (link is external)
ibm -- tivoli_monitoring	IBM Tivoli Monitoring 6.2 and 6.3 is vulnerable to possible host header injection attack that could lead to HTTP cache poisoning or firewall bypass. IBM Reference #: 1997223.	2017-03-08	4.9	CVE-2016-5933 CONFIRM (link is external)
ibm -- websphere_mq	IBM WebSphere MQ 8.0 could allow an authenticated user with queue manager permissions to cause a segmentation fault which would result in the box having to be rebooted to resume normal operations. IBM Reference #: 1998663.	2017-03-07	6.8	CVE-2016-8971 CONFIRM (link is external)
imagemagick -- imagemagick	An issue was discovered in ImageMagick 6.9.7. A specially crafted psd file could lead to a NULL pointer dereference (thus, a DoS).	2017-03-05	5.0	CVE-2017-6497 BID (link is external) CONFIRM CONFIRM (link is external)
imagemagick -- imagemagick	An issue was discovered in ImageMagick 6.9.7. Incorrect TGA files could trigger assertion failures, thus leading to DoS.	2017-03-05	4.3	CVE-2017-6498 BID (link is external) CONFIRM CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	An issue was discovered in Magick++ in ImageMagick 6.9.7. A specially crafted file creating a nested exception could lead to a memory leak (thus, a DoS).	2017-03-05	4.3	CVE-2017-6499 BID (link is external) CONFIRM CONFIRM (link is external) CONFIRM

imagemagick -- imagemagick	An issue was discovered in ImageMagick 6.9.7. A specially crafted sun file triggers a heap-based buffer over-read.	2017-03-05	4.3	CVE-2017-6500 BID (link is external) CONFIRM CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
imagemagick -- imagemagick	An issue was discovered in ImageMagick 6.9.7. A specially crafted xcf file could lead to a NULL pointer dereference.	2017-03-05	4.3	CVE-2017-6501 BID (link is external) CONFIRM CONFIRM (link is external)
imagemagick -- imagemagick	An issue was discovered in ImageMagick 6.9.7. A specially crafted webp file could lead to a file-descriptor leak in libmagickcore (thus, a DoS).	2017-03-05	4.3	CVE-2017-6502 CONFIRM (link is external)
intel -- quickassist_technology_engine	The RSA-CRT implementation in the Intel QuickAssist Technology (QAT) Engine for OpenSSL versions prior to 0.5.19 may allow remote attackers to obtain private RSA keys by conducting a Lenstra side-channel attack.	2017-03-07	5.0	CVE-2017-5681 CONFIRM (link is external)
inter-mediator_project -- inter-mediator	Multiple Cross-Site Scripting (XSS) issues were discovered in INTER-Mediator 5.5. The vulnerabilities exist due to insufficient filtration of user-supplied data (c and cred) passed to the "INTER-Mediator-master/Auth_Support/PasswordReset/resetpassword.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-05	4.3	CVE-2017-6484 CONFIRM (link is external)
irssi -- irssi	The nickcmp function in Irssi before 0.8.21 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a message without a nick.	2017-03-03	5.0	CVE-2017-5193 MLIST (link is external) BID (link is external) CONFIRM
irssi -- irssi	Use-after-free vulnerability in Irssi before 0.8.21 allows remote attackers to cause a denial of service (crash) via an invalid nick message.	2017-03-03	5.0	CVE-2017-5194 MLIST (link is external) BID (link is external)

				CONFIRM
irssi -- irssi	Irssi 0.8.17 before 0.8.21 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted ANSI x8 color code.	2017-03-03	5.0	CVE-2017-5195 MLIST (link is external) BID (link is external) CONFIRM
irssi -- irssi	Irssi 0.8.18 before 0.8.21 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via vectors involving strings that are not UTF8.	2017-03-03	5.0	CVE-2017-5196 MLIST (link is external) BID (link is external) CONFIRM
irssi -- irssi	Irssi before 0.8.21 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a string containing a formatting sequence (%[) without a closing bracket (]).	2017-03-03	5.0	CVE-2017-5356 MLIST (link is external) MLIST (link is external) BID (link is external) MISC CONFIRM
lenovo -- thinkserver_firmware	Reset to default settings may occur in Lenovo ThinkServer TSM RD350, RD450, RD550, RD650, TD350 during a prolonged broadcast storm in TSM versions earlier than 3.77.	2017-03-03	5.0	CVE-2016-8236 CONFIRM (link is external)
libimobiledevice -- libplist	The parse_dict_node function in bplist.c in libplist allows attackers to cause a denial of service (out-of-bounds heap read and crash) via a crafted file.	2017-03-03	4.3	CVE-2017-5834 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
libimobiledevice -- libplist	libplist allows attackers to cause a denial of service (large memory allocation and crash) via vectors involving an offset size of zero.	2017-03-03	5.0	CVE-2017-5835 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
libimobiledevice -- libplist	The plist_free_data function in plist.c in libplist allows attackers to cause a denial of service (crash) via vectors involving an integer node that is treated	2017-03-03	5.0	CVE-2017-5836 MLIST (link is external) MLIST (link is

	as a PLIST_KEY and then triggers an invalid free.			external) BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm power driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as High because it could be used to access sensitive data without explicit user permission. Product: Android. Versions: Kernel-3.10. Android ID: A-33745862. References: QC-CR#1035099.	2017-03-07	4.3	CVE-2016-8483 MISC (link is external) CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the NVIDIA GPU driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as High because it could be used to access sensitive data without explicit user permission. Product: Android. Versions: Kernel-3.18. Android ID: A-33245849. References: N-CVE-2017-0334.	2017-03-07	4.3	CVE-2017-0334 CONFIRM (link is external)
linux -- linux_kernel	An information disclosure vulnerability in the NVIDIA GPU driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as High because it could be used to access sensitive data without explicit user permission. Product: Android. Versions: Kernel-3.18. Android ID: A-33042679. References: N-CVE-2017-0336.	2017-03-07	4.3	CVE-2017-0336 CONFIRM (link is external)
mail-masta_project -- mail-masta	A SQL injection issue is exploitable, with WordPress admin access, in the Mail Masta (aka mail-masta) plugin 1.0 for WordPress. This affects ./inc/campaign/view-campaign-list.php with the GET Parameter: id.	2017-03-09	6.5	CVE-2017-6570 MISC (link is external)
mail-masta_project -- mail-masta	A SQL injection issue is exploitable, with WordPress admin access, in the Mail Masta (aka mail-masta) plugin 1.0 for WordPress. This affects ./inc/campaign/view-campaign.php with the GET Parameter: id.	2017-03-09	6.5	CVE-2017-6571 MISC (link is external)

mail-masta_project -- mail-masta	A SQL injection issue is exploitable, with WordPress admin access, in the Mail Masta (aka mail-masta) plugin 1.0 for WordPress. This affects ./inc/lists/add_member.php with the GET Parameter: filter_list.	2017-03-09	6.5	CVE-2017-6572 MISC (link is external)
mail-masta_project -- mail-masta	A SQL injection issue is exploitable, with WordPress admin access, in the Mail Masta (aka mail-masta) plugin 1.0 for WordPress. This affects ./inc/lists/edit-list.php with the GET Parameter: id.	2017-03-09	6.5	CVE-2017-6573 MISC (link is external)
mail-masta_project -- mail-masta	A SQL injection issue is exploitable, with WordPress admin access, in the Mail Masta (aka mail-masta) plugin 1.0 for WordPress. This affects ./inc/lists/edit_member.php with the GET Parameter: filter_list.	2017-03-09	6.5	CVE-2017-6574 MISC (link is external)
mail-masta_project -- mail-masta	A SQL injection issue is exploitable, with WordPress admin access, in the Mail Masta (aka mail-masta) plugin 1.0 for WordPress. This affects ./inc/lists/edit_member.php with the GET Parameter: member_id.	2017-03-09	6.5	CVE-2017-6575 MISC (link is external)
mail-masta_project -- mail-masta	A SQL injection issue is exploitable, with WordPress admin access, in the Mail Masta (aka mail-masta) plugin 1.0 for WordPress. This affects ./inc/campaign/campaign-delete.php with the GET Parameter: id.	2017-03-09	6.5	CVE-2017-6576 MISC (link is external)
mail-masta_project -- mail-masta	A SQL injection issue is exploitable, with WordPress admin access, in the Mail Masta (aka mail-masta) plugin 1.0 for WordPress. This affects ./inc/subscriber_list.php with the POST Parameter: list_id.	2017-03-09	6.5	CVE-2017-6577 MISC (link is external)
mail-masta_project -- mail-masta	A SQL injection issue is exploitable, with WordPress admin access, in the Mail Masta (aka mail-masta) plugin 1.0 for WordPress. This affects ./inc/subscriber_list.php with the POST Parameter: subscriber_email.	2017-03-09	6.5	CVE-2017-6578 MISC (link is external)
mangoswebv4_project -- mangoswebv4	paintballrefjosh/MaNGOSWebV4 before 4.0.8 is vulnerable to a reflected XSS in install/index.php (step parameter).	2017-03-05	4.3	CVE-2017-6478 BID (link is external) CONFIRM (link is external)

				CONFIRM (link is external)
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in bug_change_status_page.php in MantisBT before 1.3.7 and 2.x before 2.2.1 allows remote attackers to inject arbitrary JavaScript via the 'action_type' parameter.	2017-03-09	4.3	CVE-2017-6797 CONFIRM CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
mantisbt -- mantisbt	A cross-site scripting (XSS) vulnerability in view_filters_page.php in MantisBT before 2.2.1 allows remote attackers to inject arbitrary JavaScript via the 'view_type' parameter.	2017-03-10	4.3	CVE-2017-6799 CONFIRM CONFIRM (link is external) CONFIRM (link is external)
matrixssl -- matrixssl	MatrixSSL before 3.8.7, when the DHE_RSA based cipher suite is supported, makes it easier for remote attackers to obtain RSA private key information by conducting a Lenstra side-channel attack.	2017-03-03	4.3	CVE-2016-6882 MLIST (link is external) MISC (link is external) CONFIRM (link is external) MISC (link is external)
matrixssl -- matrixssl	MatrixSSL before 3.8.3 configured with RSA Cipher Suites allows remote attackers to obtain sensitive information via a Bleichenbacher variant attack.	2017-03-03	4.3	CVE-2016-6883 MLIST (link is external) CONFIRM (link is external)
matrixssl -- matrixssl	TLS cipher suites with CBC mode in TLS 1.1 and 1.2 in MatrixSSL before 3.8.3 allow remote attackers to cause a denial of service (out-of-bounds read) via a crafted message.	2017-03-03	4.3	CVE-2016-6884 MLIST (link is external) CONFIRM (link is external)
openbsd -- openbsd	The mmap extension __MAP_NOFAULT in OpenBSD 5.8 and 5.9 allows attackers to cause a denial of service (kernel panic and crash) via a large size value.	2017-03-07	4.9	CVE-2016-6239 CONFIRM CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external)
openbsd -- openbsd	OpenBSD 5.8 and 5.9 allows local users to cause a denial of service (assertion failure and kernel panic) via a large ident value in a kevent system call.	2017-03-07	4.9	CVE-2016-6242 CONFIRM CONFIRM MLIST (link is external)

				MLIST (link is external) BID (link is external)
openbsd -- openbsd	thrsleep in kern/kern_synch.c in OpenBSD 5.8 and 5.9 allows local users to cause a denial of service (kernel panic) via a crafted value in the tsp parameter of the __thrsleep system call.	2017-03-07	4.9	CVE-2016-6243 CONFIRM CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external)
openbsd -- openbsd	OpenBSD 5.8 and 5.9 allows local users to cause a denial of service (kernel panic) via a large size in a getdents system call.	2017-03-07	4.9	CVE-2016-6245 CONFIRM CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external)
openbsd -- openbsd	OpenBSD 5.8 and 5.9 allows certain local users with kern.usermount privileges to cause a denial of service (kernel panic) by mounting a tmpfs with a VNOVAL in the (1) username, (2) groupname, or (3) device name of the root node.	2017-03-07	4.9	CVE-2016-6246 CONFIRM CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external)
openbsd -- openbsd	OpenBSD 5.8 and 5.9 allows certain local users to cause a denial of service (kernel panic) by unmounting a filesystem with an open vnode on the mnt_vnodelist.	2017-03-07	4.9	CVE-2016-6247 CONFIRM CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external)
openbsd -- openbsd	OpenBSD 5.8 and 5.9 allows local users to cause a denial of service (NULL pointer dereference and panic) via a sysctl call with a path starting with 10,9.	2017-03-07	4.9	CVE-2016-6350 CONFIRM CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external)

openbsd -- openbsd	Integer overflow in the uvm_map_isavail function in uvm/uvm_map.c in OpenBSD 5.9 allows local users to cause a denial of service (kernel panic) via a crafted mmap call, which triggers the new mapping to overlap with an existing mapping.	2017-03-07	4.9	CVE-2016-6522 CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external)
owncloud -- owncloud	The password reset functionality in ownCloud Server before 8.1.11, 8.2.x before 8.2.9, 9.0.x before 9.0.7, and 9.1.x before 9.1.3 sends different error messages depending on whether the username is valid, which allows remote attackers to enumerate user names via a large number of password reset attempts.	2017-03-03	4.3	CVE-2017-5865 BID (link is external) CONFIRM
owncloud -- owncloud	The autocomplete feature in the E-Mail share dialog in ownCloud Server before 8.1.11, 8.2.x before 8.2.9, 9.0.x before 9.0.7, and 9.1.x before 9.1.3 allows remote authenticated users to obtain sensitive information via unspecified vectors.	2017-03-03	4.0	CVE-2017-5866 BID (link is external) CONFIRM
owncloud -- owncloud	ownCloud Server before 8.1.11, 8.2.x before 8.2.9, 9.0.x before 9.0.7, and 9.1.x before 9.1.3 allows remote authenticated users to cause a denial of service (server hang and logfile flooding) via a one bit BMP file.	2017-03-03	4.0	CVE-2017-5867 BID (link is external) CONFIRM
php-calendar -- php-calendar	A Cross-Site Scripting (XSS) issue was discovered in php-calendar before 2017-03-03. The vulnerability exists due to insufficient filtration of user-supplied data (errorMsg) passed to the "php-calendar-master/error.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-05	4.3	CVE-2017-6485 CONFIRM (link is external)
phpipam -- phpipam	Multiple Cross-Site Scripting (XSS) issues were discovered in phpipam 1.2. The vulnerabilities exist due to insufficient filtration of user-supplied data passed to several pages (instructions in app/admin/instructions/preview.php; subnetId in app/admin/powerDNS/refresh-ptr-records.php). An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable	2017-03-05	4.3	CVE-2017-6481 BID (link is external) CONFIRM (link is external)

	website.			
plone -- plone	Directory traversal vulnerability in Plone CMS 5.x through 5.0.6 and 4.2.x through 4.3.11 allows remote administrators to read arbitrary files via a .. (dot dot) in the path parameter in a getFile action to Plone/++theme+ +barceloneta/@@plone.resourceeditor.filemanager -actions.	2017-03-07	4.0	CVE-2016-7135 MISC (link is external) FULLDISC MLIST (link is external) MLIST (link is external) BUGTRAQ (link is external) BID (link is external) CONFIRM
plone -- plone	z3c.form in Plone CMS 5.x through 5.0.6 and 4.x through 4.3.11 allows remote attackers to conduct cross-site scripting (XSS) attacks via a crafted GET request.	2017-03-07	4.3	CVE-2016-7136 MISC (link is external) FULLDISC MLIST (link is external) MLIST (link is external) BUGTRAQ (link is external) BID (link is external) CONFIRM
plone -- plone	Multiple open redirect vulnerabilities in Plone CMS 5.x through 5.0.6, 4.x through 4.3.11, and 3.3.x through 3.3.6 allow remote attackers to redirect users to arbitrary web sites and conduct phishing attacks via a URL in the referer parameter to (1) %2b %2bgroupdashboard%2b %2bplone.dashboard1%2bgroup/ %2b/portlets.Actions or (2) folder/%2b %2bcontextportlets%2b%2bplone.footerportlets/ %2b /portlets.Actions or the (3) came_from parameter to /login_form.	2017-03-07	5.8	CVE-2016-7137 MISC (link is external) FULLDISC MLIST (link is external) MLIST (link is external) BUGTRAQ (link is external) BID (link is external) CONFIRM
plone -- plone	Cross-site scripting (XSS) vulnerability in the URL checking infrastructure in Plone CMS 5.x through 5.0.6, 4.x through 4.3.11, and 3.3.x through 3.3.6 allows remote attackers to inject arbitrary web script or HTML via a crafted URL.	2017-03-07	4.3	CVE-2016-7138 MISC (link is external) FULLDISC MLIST (link is external) MLIST (link is external) BUGTRAQ

				(link is external) BID (link is external) CONFIRM
plone -- plone	Cross-site scripting (XSS) vulnerability in an unspecified page template in Plone CMS 5.x through 5.0.6, 4.x through 4.3.11, and 3.3.x through 3.3.6 allows remote attackers to inject arbitrary web script or HTML via unknown vectors.	2017-03-07	4.3	CVE-2016-7139 MISC (link is external) FULLDISC MLIST (link is external) MLIST (link is external) BUGTRAQ (link is external) BID (link is external) CONFIRM
plone -- plone	Multiple cross-site scripting (XSS) vulnerabilities in the ZMI page in Zope2 in Plone CMS 5.x through 5.0.6, 4.x through 4.3.11, and 3.3.x through 3.3.6 allow remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2017-03-07	4.3	CVE-2016-7140 MISC (link is external) FULLDISC MLIST (link is external) MLIST (link is external) BUGTRAQ (link is external) BID (link is external) CONFIRM
pysaml2_project -- pysaml2	PySAML2 allows remote attackers to conduct XML external entity (XXE) attacks via a crafted SAML XML request or response.	2017-03-03	6.8	CVE-2016-10127 MLIST (link is external) BID (link is external) MISC MISC (link is external) MISC (link is external) MISC (link is external)
qbittorrent -- qbittorrent	WebUI in qBittorrent before 3.3.11 did not escape many values, which could potentially lead to XSS.	2017-03-05	4.3	CVE-2017-6503 CONFIRM (link is external) CONFIRM
qbittorrent -- qbittorrent	WebUI in qBittorrent before 3.3.11 did not set the X-Frame-Options header, which could potentially lead	2017-03-05	4.3	CVE-2017-6504 CONFIRM (link is external)

	to clickjacking.			CONFIRM
qt -- qxmlsimplereader	Stack-based buffer overflow in QXmlSimpleReader in Qt 4.8.5 allows remote attackers to cause a denial of service (application crash) via a xml file with multiple nested open tags.	2017-03-07	4.3	CVE-2016-10040 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
reasoncms_project -- reasoncms	A Cross-Site Scripting (XSS) issue was discovered in reasoncms before 4.7.1. The vulnerability exists due to insufficient filtration of user-supplied data (nyroModalSel) passed to the "reasoncms-master/www/nyroModal/demoSent.php" URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-05	4.3	CVE-2017-6486 CONFIRM (link is external) CONFIRM (link is external)
revive-adserver -- revive_adserver	Session fixation vulnerability in the forgot password mechanism in Revive Adserver before 4.0.1, when setting a new password, allows remote attackers to hijack web sessions via the session ID.	2017-03-03	5.5	CVE-2017-5831 MLIST (link is external) BID (link is external) CONFIRM (link is external)
revive-adserver -- revive_adserver	Cross-site scripting (XSS) vulnerability in the invocation code generation for interstitial zones in Revive Adserver before 4.0.1 allows remote attackers to inject arbitrary web script or HTML via unspecified parameters.	2017-03-03	4.3	CVE-2017-5833 MLIST (link is external) BID (link is external) CONFIRM (link is external)
sanadata -- sanacms	Cross-site scripting (XSS) vulnerability in /sanadata/seo/index.asp in SANADATA SanaCMS 7.3 allows remote attackers to inject arbitrary web script or HTML via the txtFrom parameter.	2017-03-07	4.3	CVE-2017-6518 MISC (link is external)
silverstripe -- silverstripe	There is XSS in SilverStripe CMS before 3.4.4 and 3.5.x before 3.5.2. The attack vector is a page name. An example payload is a crafted JavaScript event handler within a malformed SVG element.	2017-03-06	4.3	CVE-2017-5197 BID (link is external) CONFIRM
telaxus -- epesi	Multiple Cross-Site Scripting (XSS) issues were discovered in EPESI 1.8.1.1. The vulnerabilities exist	2017-03-05	4.3	CVE-2017-6487 BID (link is external)

	due to insufficient filtration of user-supplied data (state, element, id, tab, cid) passed to the "EPESI-master/modules/Utils/RecordBrowser/favorites.php " URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.			CONFIRM (link is external)
telaxus -- epesi	Multiple Cross-Site Scripting (XSS) issues were discovered in EPESI 1.8.1.1. The vulnerabilities exist due to insufficient filtration of user-supplied data (visible, tab, cid) passed to the EPESI-master/modules/Utils/RecordBrowser/Filters/save_filters.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-05	4.3	CVE-2017-6488 CONFIRM (link is external)
telaxus -- epesi	Multiple Cross-Site Scripting (XSS) issues were discovered in EPESI 1.8.1.1. The vulnerabilities exist due to insufficient filtration of user-supplied data (element, state, cat, id, cid) passed to the EPESI-master/modules/Utils/Watchdog/subscribe.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-05	4.3	CVE-2017-6489 CONFIRM (link is external)
telaxus -- epesi	Multiple Cross-Site Scripting (XSS) issues were discovered in EPESI 1.8.1.1. The vulnerabilities exist due to insufficient filtration of user-supplied data (cid, value, element, mode, tab, form_name, id) passed to the EPESI-master/modules/Utils/RecordBrowser/grid.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-05	4.3	CVE-2017-6490 CONFIRM (link is external)
telaxus -- epesi	Multiple Cross-Site Scripting (XSS) issues were discovered in EPESI 1.8.1.1. The vulnerabilities exist due to insufficient filtration of user-supplied data (tooltip_id, callback, args, cid) passed to the EPESI-master/modules/Utils/Tooltip/req.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-05	4.3	CVE-2017-6491 CONFIRM (link is external)

tenable -- nessus	Tenable Nessus before 6.10.2 (as used alone or in Tenable Appliance before 4.5.0) was found to contain a flaw that allowed a remote, authenticated attacker to upload a crafted file that could be written to anywhere on the system. This could be used to subsequently gain elevated privileges on the system (e.g., after a reboot). This issue only affects installations on Windows.	2017-03-08	6.0	CVE-2017-6543 CONFIRM (link is external)
umbraco -- umbraco	The Page_Load function in Umbraco.Web/umbraco.presentation/umbraco/dashboard/FeedProxy.aspx.cs in Umbraco before 7.4.0 allows remote attackers to conduct server-side request forgery (SSRF) attacks via the url parameter.	2017-03-03	4.3	CVE-2015-8813 CONFIRM MLIST (link is external) MLIST (link is external) MLIST (link is external) MLIST (link is external) CONFIRM (link is external)
umbraco -- umbraco	Umbraco before 7.4.0 allows remote attackers to bypass anti-forgery security measures and conduct cross-site request forgery (CSRF) attacks as demonstrated by editing user account information in the templates.asmx.cs file.	2017-03-03	6.8	CVE-2015-8814 CONFIRM MLIST (link is external) CONFIRM (link is external)
umbraco -- umbraco	Multiple cross-site scripting (XSS) vulnerabilities in Umbraco before 7.4.0 allow remote attackers to inject arbitrary web script or HTML via the name parameter to (1) the media page, (2) the developer data edit page, or (3) the form page.	2017-03-03	5.0	CVE-2015-8815 CONFIRM MLIST (link is external)
webkit -- webkit	The regex code in Webkit 2.4.11 allows remote attackers to cause a denial of service (memory consumption) as demonstrated in a large number of ($ (open parenthesis and dollar) followed by {-2,16} and a large number of +) (plus close parenthesis).	2017-03-07	5.0	CVE-2016-9643 MLIST (link is external) MLIST (link is external) BID (link is external)
webpagetest_project -- webpagetest	A Cross-Site Scripting (XSS) issue was discovered in webpagetest 3.0. The vulnerability exists due to insufficient filtration of user-supplied data (benchmark) passed to the webpagetest-master/www/benchmarks/view.php URL. An	2017-03-08	4.3	CVE-2017-6533 CONFIRM (link is external)

	attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.			
webpagetest_project -- webpagetest	A Cross-Site Scripting (XSS) issue was discovered in webpagetest 3.0. The vulnerability exists due to insufficient filtration of user-supplied data (pssid) passed to the webpagetest-master/www/pss.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-08	4.3	CVE-2017-6534 CONFIRM (link is external)
webpagetest_project -- webpagetest	Multiple Cross-Site Scripting (XSS) issues were discovered in webpagetest 3.0. The vulnerabilities exist due to insufficient filtration of user-supplied data (benchmark, url) passed to the webpagetest-master/www/benchmarks/trendurl.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-08	4.3	CVE-2017-6535 CONFIRM (link is external)
webpagetest_project -- webpagetest	Multiple Cross-Site Scripting (XSS) issues were discovered in webpagetest 3.0. The vulnerabilities exist due to insufficient filtration of user-supplied data (url, pssid) passed to the webpagetest-master/www/weblite.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-08	4.3	CVE-2017-6536 CONFIRM (link is external)
webpagetest_project -- webpagetest	A Cross-Site Scripting (XSS) issue was discovered in webpagetest 3.0. The vulnerability exists due to insufficient filtration of user-supplied data (bgcolor) passed to the webpagetest-master/www/video/view.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-08	4.3	CVE-2017-6537 CONFIRM (link is external)
webpagetest_project -- webpagetest	A Cross-Site Scripting (XSS) issue was discovered in webpagetest 3.0. The vulnerability exists due to insufficient filtration of user-supplied data (video) passed to the webpagetest-master/www/speedindex/index.php URL. An attacker could execute arbitrary HTML and script	2017-03-08	4.3	CVE-2017-6538 CONFIRM (link is external)

	code in a browser in the context of the vulnerable website.			
webpagetest_project -- webpagetest	Multiple Cross-Site Scripting (XSS) issues were discovered in webpagetest 3.0. The vulnerabilities exist due to insufficient filtration of user-supplied data (benchmark, time) passed to the webpagetest-master/www/benchmarks/delta.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-08	4.3	CVE-2017-6539 CONFIRM (link is external)
webpagetest_project -- webpagetest	Multiple Cross-Site Scripting (XSS) issues were discovered in webpagetest 3.0. The vulnerabilities exist due to insufficient filtration of user-supplied data (configs) passed to the webpagetest-master/www/benchmarks/compare.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-08	4.3	CVE-2017-6540 CONFIRM (link is external)
webpagetest_project -- webpagetest	Multiple Cross-Site Scripting (XSS) issues were discovered in webpagetest 3.0. The vulnerabilities exist due to insufficient filtration of user-supplied data (benchmark, time) passed to the webpagetest-master/www/benchmarks/viewtest.php URL. An attacker could execute arbitrary HTML and script code in a browser in the context of the vulnerable website.	2017-03-08	4.3	CVE-2017-6541 CONFIRM (link is external)
wireshark -- wireshark	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is a Netscaler file parser infinite loop, triggered by a malformed capture file. This was addressed in wiretap/netscaler.c by changing the restrictions on file size.	2017-03-03	5.0	CVE-2017-6467 CONFIRM CONFIRM CONFIRM
wireshark -- wireshark	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is a NetScaler file parser crash, triggered by a malformed capture file. This was addressed in wiretap/netscaler.c by validating the relationship between pages and records.	2017-03-03	5.0	CVE-2017-6468 CONFIRM CONFIRM CONFIRM
wireshark -- wireshark	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is an LDSS dissector crash, triggered by packet	2017-03-03	5.0	CVE-2017-6469 CONFIRM CONFIRM

	injection or a malformed capture file. This was addressed in epan/dissectors/packet-ldss.c by ensuring that memory is allocated for a certain data structure.			CONFIRM
wireshark -- wireshark	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is a WSP infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-wsp.c by validating the capability length.	2017-03-03	5.0	CVE-2017-6471 CONFIRM CONFIRM CONFIRM
wireshark -- wireshark	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is an RTMPT dissector infinite loop, triggered by packet injection or a malformed capture file. This was addressed in epan/dissectors/packet-rtmpt.c by properly incrementing a certain sequence value.	2017-03-03	5.0	CVE-2017-6472 CONFIRM CONFIRM CONFIRM
wireshark -- wireshark	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is a K12 file parser crash, triggered by a malformed capture file. This was addressed in wiretap/k12.c by validating the relationships between lengths and offsets.	2017-03-03	5.0	CVE-2017-6473 CONFIRM CONFIRM CONFIRM
wireshark -- wireshark	In Wireshark 2.2.0 to 2.2.4 and 2.0.0 to 2.0.10, there is a NetScaler file parser infinite loop, triggered by a malformed capture file. This was addressed in wiretap/netscaler.c by validating record sizes.	2017-03-03	5.0	CVE-2017-6474 CONFIRM CONFIRM CONFIRM
wp_markdown_editor_project -- wp_markdown_editor	A Stored XSS Vulnerability exists in the WP Markdown Editor (aka wp-markdown-editor) plugin 2.0.3 for WordPress. An example attack vector is a crafted IMG element in Add New Post or Edit Post.	2017-03-10	4.3	CVE-2017-6804 MISC (link is external)
wuhu_project -- wuhu	Gargaj/wuhu through 2017-03-08 is vulnerable to a reflected XSS in wuhu-master/www_admin/users.php (id parameter).	2017-03-08	4.3	CVE-2017-6544 CONFIRM (link is external)
zoneminder -- zoneminder	Cross-site scripting (XSS) vulnerability in Zoneminder 1.30 and earlier allows remote attackers to inject arbitrary web script or HTML via the format parameter in a download log request to index.php.	2017-03-03	4.3	CVE-2016-10201 MLIST (link is external) MISC (link is external)
zoneminder -- zoneminder	Cross-site scripting (XSS) vulnerability in Zoneminder 1.30 and earlier allows remote	2017-03-03	4.3	CVE-2016-10202 MLIST (link is

	attackers to inject arbitrary web script or HTML via the path info to index.php.			external) MISC (link is external)
zoneminder -- zoneminder	Cross-site scripting (XSS) vulnerability in Zoneminder 1.30 and earlier allows remote attackers to inject arbitrary web script or HTML via the name when creating a new monitor.	2017-03-03	4.3	CVE-2016-10203 MLIST (link is external) MISC (link is external)
zoneminder -- zoneminder	Cross-site request forgery (CSRF) vulnerability in Zoneminder 1.30 and earlier allows remote attackers to hijack the authentication of users for requests that change passwords and possibly have unspecified other impact as demonstrated by a crafted user action request to index.php.	2017-03-03	6.8	CVE-2016-10206 MLIST (link is external) MISC (link is external)

Low Severity Vulnerabilities

The Primary Vendor --- Product	Description	Date Published	CVSS Score	The CVE Identity
cmsmadesimple -- cms_made_simple	Cross-site scripting (XSS) vulnerability in /admin/moduleinterface.php in CMS Made Simple 2.1.6 allows remote authenticated users to inject arbitrary web script or HTML via the m1_description parameter (aka "Design Manager > Categories > Category Description").	2017-03-09	3.5	CVE-2017-6555 MISC (link is external)
cmsmadesimple -- cms_made_simple	Cross-site scripting (XSS) vulnerability in CMS Made Simple (CMSMS) 2.1.6 allows remote authenticated users to inject arbitrary web script or HTML via the "adminpage > sitesetting > General Settings > globalmetadata" field.	2017-03-09	3.5	CVE-2017-6556 MISC (link is external)
google -- android	A denial of service vulnerability in Setup Wizard could allow a local attacker to require Google account sign-in after a factory reset. This issue is	2017-03-07	2.1	CVE-2017-0498 MISC (link is external)

	rated as Moderate because it may require a factory reset to repair the device. Product: Android. Versions: 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-30352311.			
google -- android	An information disclosure vulnerability in the MediaTek video codec 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: N/A. Android ID: A-32370398. References: M-ALPS03069985.	2017-03-07	2.6	CVE-2017-0532 MISC (link is external)
ibm -- cognos_business_intelligence	IBM Cognos Server 10.1.1 and 10.2 stores highly sensitive information in log files that could be read by a local user. IBM Reference #: 1999671.	2017-03-08	2.1	CVE-2016-9985 CONFIRM (link is external)
ibm -- db2	IBM DB2 for Linux, UNIX and Windows (includes DB2 Connect Server) 10.1, 10.5, and 11.1 could allow an authenticated attacker with specialized access to tables that they should not be permitted to view. IBM Reference #: 1999515.	2017-03-08	3.5	CVE-2017-1150 CONFIRM (link is external) BID (link is external)
ibm -- maximo_asset_management	IBM Maximo Asset Management 7.1, 7.5, and 7.6 could allow a local attacker to obtain sensitive information using HTTP Header Injection. IBM Reference #: 1998053.	2017-03-07	1.9	CVE-2017-1124 CONFIRM (link is external) BID (link is external)
ibm -- qradar_security_information_and_event_manager	IBM QRadar 7.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: 1999534.	2017-03-07	3.5	CVE-2017-1133 CONFIRM (link is external)
ibm -- urbancode_deploy	IBM UrbanCode Deploy 6.1 and 6.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM Reference #: C1000264.	2017-03-08	3.5	CVE-2016-9006 CONFIRM (link is external)
ibm -- websphere_commerce	IBM WebSphere Commerce Enterprise, Professional, Express, and Developer 7.0 and 8.0 is vulnerable to information disclosure vulnerability. A local user	2017-03-08	1.9	CVE-2016-5894 CONFIRM (link is external) BID (link is

	could view a plain text password in a Unix console. IBM Reference #: 1997408.			external)
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm camera 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-32709702. References: QC-CR#518731.	2017-03-07	2.6	CVE-2016-8413 MISC (link is external) CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm video 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-3.18. Android ID: A-32510746. References: QC-CR#1088206.	2017-03-07	2.6	CVE-2016-8416 MISC (link is external) CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm camera 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-32720522. References: QC-CR#1090007.	2017-03-07	2.6	CVE-2016-8477 MISC (link is external) CONFIRM CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm video 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-3.18. Android ID: A-32511270. References: QC-CR#1088206.	2017-03-07	2.6	CVE-2016-8478 MISC (link is external) CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm camera driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Low because	2017-03-07	2.6	CVE-2017-0452 MISC (link is external)

	it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-32873615. References: QC-CR#1093693.			
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-3.18. Android ID: A-32644895. References: QC-CR#1091939.	2017-03-07	2.6	CVE-2017-0459 MISC (link is external) CONFIRM
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-32073794. References: QC-CR#1100132.	2017-03-07	2.6	CVE-2017-0461 MISC (link is external) CONFIRM
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-32877245. References: QC-CR#1087469.	2017-03-07	2.6	CVE-2017-0531 MISC (link is external) CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm video 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-3.18. Android ID: A-32509422. References: QC-CR#1088206.	2017-03-07	2.6	CVE-2017-0533 MISC (link is external) CONFIRM
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm video driver could enable a local malicious application to access data outside of its	2017-03-07	2.6	CVE-2017-0534 MISC (link is external) CONFIRM

	permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-32508732. References: QC-CR#1088206.			
linux -- linux_kernel	An information disclosure vulnerability in the HTC sound codec 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. Android ID: A-33547247.	2017-03-07	2.6	CVE-2017-0535 MISC (link is external)
linux -- linux_kernel	An information disclosure vulnerability in the Synaptics touchscreen 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-33555878.	2017-03-07	2.6	CVE-2017-0536 MISC (link is external)
linux -- linux_kernel	An information disclosure vulnerability in the kernel USB gadget 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-3.18. Android ID: A-31614969.	2017-03-07	2.6	CVE-2017-0537 MISC (link is external)
revive-adserver -- revive_adserver	Cross-site scripting (XSS) vulnerability in Revive Adserver before 4.0.1 allows remote authenticated users to inject arbitrary web script or HTML via the user's email address.	2017-03-03	3.5	CVE-2017-5832 MLIST (link is external) BID (link is external) CONFIRM (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