Vulnerability Summary for the Week of February 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**
dotnetnuke -- dotnetnuke	The installation wizard in DotNetNuke (DNN) before 7.4.1 allows remote attackers to reinstall the application and gain SuperUser access via a direct request to Install/InstallWizard.aspx.	2017-02-06	7.5	CVE-2015-2794 CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) EXPLOIT-DB (link is external)
exponentcms -- exponent_cms	Multiple SQL injection vulnerabilities in Exponent CMS before 2.4.0 allow remote attackers to execute arbitrary SQL commands via the (1) id parameter in an activate_address address controller action, (2) title parameter in a show blog controller action, or (3) content_id parameter in a showComments expComment controller action.	2017-02-07	7.5	CVE-2016-7400 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
exponentcms -- exponent_cms	An issue was discovered in Exponent CMS 2.4.1. This is a blind SQL injection that can be exploited by un-authenticated users via an HTTP GET request and which can be used to dump	2017-02-06	7.5	CVE-2017-5879 BID (link is external) MISC (link is external)

	database data out to a malicious server, using an out-of-band technique, such as select_loadfile(). The vulnerability affects source_selector.php and the following parameter: src.			
google -- android	Race condition in the ip4_datagram_release_cb function in net/ipv4/datagram.c in the Linux kernel before 3.15.2 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging incorrect expectations about locking during multithreaded access to internal data structures for IPv4 UDP sockets.	2017-02-07	7.2	CVE-2014-9914 CONFIRM CONFIRM (link is external) CONFIRM BID (link is external) CONFIRM (link is external)
google -- android	The aio_mount function in fs/aio.c in the Linux kernel before 4.7.7 does not properly restrict execute access, which makes it easier for local users to bypass intended SELinux W^X policy restrictions, and consequently gain privileges, via an io_setup system call.	2017-02-07	7.2	CVE-2016-10044 CONFIRM CONFIRM (link is external) CONFIRM BID (link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in the Qualcomm crypto driver could enable a remote attacker to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of remote code execution in the context of the kernel. Product: Android. Versions: N/A. Android ID: A-32652894. References: QC-CR#1077457.	2017-02-08	10.0	CVE-2016-8418 BID (link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in Surfaceflinger 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 Surfaceflinger process. Product: Android. Versions: 7.0, 7.1.1. Android ID: A-31960359.	2017-02-08	9.3	CVE-2017-0405 BID (link is external) CONFIRM (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	2017-02-08	9.3	CVE-2017-0406 BID (link is external) CONFIRM (link is external)

	is rated as Critical due to the possibility of remote code execution within the context of the Mediaserver process. This affects the libhevc library. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32915871.			
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. This affects the libhevc library. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32873375.	2017-02-08	9.3	CVE-2017-0407 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in the Framework APIs could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-31929765.	2017-02-08	9.3	CVE-2017-0410 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in the Framework APIs 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: 7.0, 7.1.1. Android ID: A-33042690.	2017-02-08	9.3	CVE-2017-0411 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in the Framework APIs 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	2017-02-08	9.3	CVE-2017-0412 BID (link is external) CONFIRM (link is external)

	not normally accessible to a third-party application. Product: Android. Versions: 7.0, 7.1.1. Android ID: A-33039926.			
google -- android	An elevation of privilege vulnerability in Mediaserver 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: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32706020.	2017-02-08	9.3	CVE-2017-0415 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in Audioserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32886609.	2017-02-08	9.3	CVE-2017-0416 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in Audioserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party application. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32705438.	2017-02-08	9.3	CVE-2017-0417 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in Audioserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as High because it could be used to gain local access to elevated capabilities, which are not normally accessible to a third-party	2017-02-08	9.3	CVE-2017-0418 BID (link is external) CONFIRM (link is external)

	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-32703959.			
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-32220769.	2017-02-08	9.3	CVE-2017-0419 BID (link is external) CONFIRM (link is external)
google -- android	A denial of service vulnerability in Bionic DNS could enable a remote attacker to use a specially crafted network packet to cause a device hang or reboot. This issue is rated as High due to the possibility of remote denial of service. 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-32322088.	2017-02-08	7.8	CVE-2017-0422 BID (link is external) CONFIRM (link is external)
google -- android	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 touchscreen chipset. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-33001936.	2017-02-08	7.6	CVE-2017-0434 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in the HTC touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-32769717.	2017-02-08	7.6	CVE-2017-0445 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in the HTC touchscreen driver could enable a local	2017-02-08	7.6	CVE-2017-0446 BID (link is external)

	malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-32917445.			CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in the HTC touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.18. Android ID: A-32919560.	2017-02-08	7.6	CVE-2017-0447 BID (link is external) CONFIRM (link is external)
google -- android	An elevation of privilege vulnerability in Audioserver could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as Moderate because it is mitigated by current platform configurations. Product: Android. Versions: N/A. Android ID: A-32917432.	2017-02-08	9.3	CVE-2017-0450 BID (link is external) CONFIRM (link is external)
graphicsmagick -- graphicsmagick	Buffer overflow in the MVG and SVG rendering code in GraphicsMagick 1.3.24 allows remote attackers to have unspecified impact via unknown vectors. Note: This vulnerability exists due to an incomplete patch for CVE-2016-2317.	2017-02-06	7.5	CVE-2016-7446 SUSE SUSE MLIST (link is external) BID (link is external) CONFIRM (link is external)
graphicsmagick -- graphicsmagick	Heap-based buffer overflow in the EscapeParenthesis function in GraphicsMagick before 1.3.25 allows remote attackers to have unspecified impact via unknown vectors.	2017-02-06	7.5	CVE-2016-7447 SUSE SUSE MLIST (link is external) BID (link is external) CONFIRM (link is external)
graphicsmagick -- graphicsmagick	The Utah RLE reader in GraphicsMagick before 1.3.25 allows remote attackers to cause a denial of service (CPU consumption or large memory	2017-02-06	7.8	CVE-2016-7448 SUSE SUSE MLIST (link is external)

	allocations) via vectors involving the header information and the file size.			BID (link is external) CONFIRM (link is external)
libwebp_project -- libwebp	Multiple integer overflows in libwebp allows attackers to have unspecified impact via unknown vectors.	2017-02-03	7.5	CVE-2016-9085 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) FEDORA FEDORA FEDORA GENTOO
linux -- linux_kernel	Use-after-free vulnerability in the kvm_ioctl_create_device function in virt/kvm/kvm_main.c in the Linux kernel before 4.8.13 allows host OS users to cause a denial of service (host OS crash) or possibly gain privileges via crafted ioctl calls on the /dev/kvm device.	2017-02-06	10.0	CVE-2016-10150 CONFIRM CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	The crypto scatterlist API in the Linux kernel 4.9.x before 4.9.6 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging reliance on earlier net/ceph/crypto.c code.	2017-02-06	7.2	CVE-2016-10153 CONFIRM CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18.	2017-02-08	7.6	CVE-2016-8419 BID (link is external) CONFIRM (link is external)

	Android ID: A-32454494. References: QC-CR#1087209.			
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-32451171. References: QC-CR#1087807.	2017-02-08	7.6	CVE-2016-8420 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32451104. References: QC-CR#1087797.	2017-02-08	7.6	CVE-2016-8421 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32879283. References: QC-CR#1091940.	2017-02-08	7.6	CVE-2016-8476 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Secure Execution Environment Communicator 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-31804432. References: QC-CR#1086186.	2017-02-08	7.6	CVE-2016-8480 BID (link is external) CONFIRM (link is external)

linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31906415. References: QC-CR#1078000.	2017-02-08	7.6	CVE-2016-8481 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the kernel file system 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-31495866.	2017-02-08	9.3	CVE-2017-0427 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-3.10. Android ID: A-32401526. References: N-CVE-2017-0428.	2017-02-08	9.3	CVE-2017-0428 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-3.10. Android ID: A-32636619. References: N-CVE-2017-0429.	2017-02-08	9.3	CVE-2017-0429 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the	2017-02-08	9.3	CVE-2017-0430

	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: Kernel-3.10, Kernel-3.18. Android ID: A-32838767. References: B-RB#107459.			BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the MediaTek 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-28332719.	2017-02-08	7.6	CVE-2017-0432 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Synaptics touchscreen driver could enable a local malicious application to execute arbitrary code within the context of the touchscreen chipset. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-31913571.	2017-02-08	7.6	CVE-2017-0433 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31906657. References: QC-CR#1078000.	2017-02-08	7.6	CVE-2017-0435 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product:	2017-02-08	7.6	CVE-2017-0436 BID (link is external) CONFIRM (link is external)

	Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32624661. References: QC-CR#1078000.			
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-32402310. References: QC-CR#1092497.	2017-02-08	7.6	CVE-2017-0437 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32402604. References: QC-CR#1092497.	2017-02-08	7.6	CVE-2017-0438 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32450647. References: QC-CR#1092059.	2017-02-08	7.6	CVE-2017-0439 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-33252788. References: QC-CR#1095770.	2017-02-08	7.6	CVE-2017-0440 BID (link is external) CONFIRM (link is external)

linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32872662. References: QC-CR#1095009.	2017-02-08	7.6	CVE-2017-0441 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32871330. References: QC-CR#1092497.	2017-02-08	7.6	CVE-2017-0442 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Qualcomm Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-32877494. References: QC-CR#1092497.	2017-02-08	7.6	CVE-2017-0443 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Realtek sound driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as High because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10. Android ID: A-32705232.	2017-02-08	7.6	CVE-2017-0444 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An elevation of privilege vulnerability in the Broadcom Wi-Fi driver could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is	2017-02-08	7.6	CVE-2017-0449 BID (link is external) CONFIRM (link is external)

	rated as Moderate because it first requires compromising a privileged process and is mitigated by current platform configurations. Product: Android. Versions: Kernel-3.10. Android ID: A-31707909. References: B-RB#32094.			
linux -- linux_kernel	The freelist-randomization feature in mm/slab.c in the Linux kernel 4.8.x and 4.9.x before 4.9.5 allows local users to cause a denial of service (duplicate freelist entries and system crash) or possibly have unspecified other impact in opportunistic circumstances by leveraging the selection of a large value for a random number.	2017-02-06	7.2	CVE-2017-5546 CONFIRM CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	drivers/hid/hid-corsair.c in the Linux kernel 4.9.x before 4.9.6 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	2017-02-06	7.2	CVE-2017-5547 CONFIRM CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	drivers/net/ieee802154/atusb.c in the Linux kernel 4.9.x before 4.9.6 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a DMA scatterlist.	2017-02-06	7.2	CVE-2017-5548 CONFIRM CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	Integer overflow in the vc4_get_bcl function in drivers/gpu/drm/vc4/vc4_gem.c in the VideoCore DRM driver in the Linux kernel before 4.9.7 allows local users to cause a denial of service or possibly have unspecified other impact via a crafted size value in a VC4_SUBMIT_CL ioctl call.	2017-02-06	7.2	CVE-2017-5576 CONFIRM CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)

				MLIST
msweet -- mini-xml	The mxmlDelete function in mxml-node.c in mxml 2.9, 2.7, and possibly earlier allows remote attackers to cause a denial of service (stack consumption) via crafted xml file.	2017-02-03	7.1	CVE-2016-4570 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
msweet -- mini-xml	The mxml_write_node function in mxml-file.c in mxml 2.9, 2.7, and possibly earlier allows remote attackers to cause a denial of service (stack consumption) via crafted xml file.	2017-02-03	7.1	CVE-2016-4571 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
saltstack -- salt	Salt before 2015.8.11 allows deleted minions to read or write to minions with the same id, related to caching.	2017-02-07	7.5	CVE-2016-9639 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
sendquick -- avera_sms_gateway_firmware	An issue was discovered on SendQuick Entera and Avera devices before 2HF16. Multiple Command Injection vulnerabilities allow attackers to execute arbitrary system commands.	2017-02-05	7.5	CVE-2016-10098 BID (link is external) MISC (link is external)
sendquick -- avera_sms_gateway_firmware	An issue was discovered on SendQuick Entera and Avera devices before 2HF16. The application failed to check the access control of the request which could result in an attacker being able to shutdown the system.	2017-02-05	7.8	CVE-2017-5136 BID (link is external) MISC (link is external)

Medium Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
cairographics -- cairo	Integer overflow in the write_png function in cairo 1.14.6 allows remote attackers to cause a denial of service (invalid pointer dereference) via a large svg file.	2017-02-03	4.3	CVE-2016-9082 MLIST (link is external) BID (link is external) CONFIRM CONFIRM CONFIRM (link is external)
cisco -- firepower_management_center	A vulnerability in the Policy deployment module of the Cisco Firepower Management Center (FMC) could allow an unauthenticated, remote attacker to prevent deployment of a complete and accurate rule base. More Information: CSCvb95281. Known Affected Releases: 6.1.0 6.2.0. Known Fixed Releases: 6.1.0.1 6.2.0.	2017-02-03	5.0	CVE-2017-3809 BID (link is external) CONFIRM (link is external)
cisco -- firepower_management_center	A vulnerability in Cisco Firepower System Software could allow an unauthenticated, remote attacker to maliciously bypass the appliance's ability to block certain web content, aka a URL Bypass. More Information: CSCvb93980. Known Affected Releases: 5.3.0 5.4.0 6.0.0 6.0.1 6.1.0.	2017-02-03	5.0	CVE-2017-3814 BID (link is external) CONFIRM (link is external)
cisco -- prime_service_catalog	A vulnerability in the web framework of Cisco Prime Service Catalog could allow an authenticated, remote attacker to conduct a web URL redirect attack against a user who is logged in to an affected system. More Information: CSCvb21745. Known Affected Releases: 10.0_R2_tanggula.	2017-02-03	4.9	CVE-2017-3810 BID (link is external) CONFIRM (link is external)
debian -- debian_linux	The Type_MLU_Read function in cmstypes.c in Little CMS (aka lcms2) allows remote attackers to obtain sensitive information or cause a denial of service via an image with a crafted ICC profile, which triggers an out-of-bounds heap read.	2017-02-03	5.8	CVE-2016-10165 SUSE DEBIAN MLIST (link is external) MLIST (link is external) BID (link is external)

				CONFIRM (link is external)
debian -- debian_linux	Integer overflow in the writeBufferToSeparateStrips function in tiffcrop.c in LibTIFF before 4.0.7 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted tif file.	2017-02-06	4.3	CVE-2016-9532 CONFIRM DEBIAN MLIST (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external) GENTOO
dotcms -- dotcms	XSS was discovered in dotCMS 3.7.0, with an unauthenticated attack against the /news-events/events date parameter.	2017-02-06	4.3	CVE-2017-5876 BID (link is external) MISC (link is external)
dotcms -- dotcms	XSS was discovered in dotCMS 3.7.0, with an unauthenticated attack against the /about-us/locations/index direction parameter.	2017-02-06	4.3	CVE-2017-5877 BID (link is external) MISC (link is external)
fedoraproject -- fedora	Heap-based buffer overflow in the color_cmyk_to_rgb in common/color.c in OpenJPEG before 2.1.1 allows remote attackers to cause a denial of service (crash) via a crafted .j2k file.	2017-02-03	4.3	CVE-2016-4796 MLIST (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) FEDORA FEDORA FEDORA FEDORA
fedoraproject -- fedora	Divide-by-zero vulnerability in the opj_tcd_init_tile function in tcd.c in OpenJPEG before 2.1.1 allows remote attackers to cause a denial of service (application crash) via a crafted jp2 file. NOTE: this issue exists because of an incorrect fix for CVE-2014-7947.	2017-02-03	4.3	CVE-2016-4797 MLIST (link is external) CONFIRM (link is external) CONFIRM (link is external) MISC (link is external) FEDORA FEDORA

				FEDORA FEDORA
fedoraproject -- fedora	The git_commit_message function in oid.c in libgit2 before 0.24.3 allows remote attackers to cause a denial of service (out-of-bounds read) via a cat-file command with a crafted object file.	2017-02-03	4.3	CVE-2016-8568 SUSE SUSE SUSE SUSE MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) FEDORA FEDORA FEDORA
fedoraproject -- fedora	The git_oid_nfmt function in commit.c in libgit2 before 0.24.3 allows remote attackers to cause a denial of service (NULL pointer dereference) via a cat-file command with a crafted object file.	2017-02-03	4.3	CVE-2016-8569 SUSE SUSE SUSE SUSE MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) FEDORA FEDORA FEDORA
fedoraproject -- fedora	Integer overflow in the js_regcomp function in regexp.c in Artifex Software, Inc. MuJS before commit b6de34ac6d8bb7dd5461c57940acfbd3ee7fd93e allows attackers to cause a denial of service (application crash) via a crafted regular expression.	2017-02-03	5.0	CVE-2016-9108 MLIST (link is external) BID (link is external) CONFIRM (link is external) FEDORA FEDORA FEDORA
gnome -- librsvg	The rsvg_pattern_fix_fallback function in rsvg-paint_server.c in librsvg2 2.40.2 allows remote	2017-02-03	4.3	CVE-2016-6163 MLIST (link is

	attackers to cause a denial of service (out-of-bounds read) via a crafted svg file.			external) MLIST (link is external) CONFIRM (link is external)
gnu -- libiberty	The demangler in GNU Libiberty allows remote attackers to cause a denial of service (infinite loop, stack overflow, and crash) via a cycle in the references of remembered mangled types.	2017-02-07	5.0	CVE-2016-6131 MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM MLIST
google -- android	A remote code execution vulnerability in libgdx 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 this library. Product: Android. Versions: 7.1.1. Android ID: A-32769670.	2017-02-08	6.8	CVE-2017-0408 BID (link is external) CONFIRM (link is external)
google -- android	A remote code execution vulnerability in libstagefright 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 this library. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-31999646.	2017-02-08	6.8	CVE-2017-0409 BID (link is external) CONFIRM (link is external)
google -- android	An information disclosure vulnerability in AOSP Messaging could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as High because it could be used to gain access to data that the application does not have access to. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32161610.	2017-02-08	4.3	CVE-2017-0413 BID (link is external) CONFIRM (link is external)
google -- android	An information disclosure vulnerability in AOSP Messaging could enable a local malicious application to bypass operating system protections that isolate application data from other	2017-02-08	4.3	CVE-2017-0414 BID (link is external) CONFIRM (link is external)

	applications. This issue is rated as High because it could be used to gain access to data that the application does not have access to. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32807795.			
google -- android	An information disclosure vulnerability in AOSP Mail could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as High because it could be used to gain access to data that the application does not have access to. 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-32615212.	2017-02-08	4.3	CVE-2017-0420 BID (link is external) CONFIRM (link is external)
google -- android	An information disclosure vulnerability in the Framework APIs could enable a local malicious application to bypass operating system protections that isolate application data from other applications. This issue is rated as High because it could be used to gain access to data that the application does not have access to. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32555637.	2017-02-08	4.3	CVE-2017-0421 BID (link is external) CONFIRM (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 is a general bypass for a user level defense in depth or exploit mitigation technology in a privileged process. Product: Android. Versions: 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32322450.	2017-02-08	4.3	CVE-2017-0424 BID (link is external) CONFIRM (link is external)
google -- android	An information disclosure vulnerability in Audioserver 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: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32720785.	2017-02-08	4.3	CVE-2017-0425 BID (link is external) CONFIRM (link is external)
google -- android	An information disclosure vulnerability in the	2017-02-08	4.3	CVE-2017-0426 BID (link is

	Filesystem 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: 7.0, 7.1.1. Android ID: A-32799236.			external) CONFIRM (link is external)
graphicsmagick -- graphicsmagick	The TIFFGetField function in coders/tiff.c in GraphicsMagick 1.3.24 allows remote attackers to cause a denial of service (out-of-bounds heap read) via a file containing an "unterminated" string.	2017-02-06	5.0	CVE-2016-7449 SUSE SUSE MLIST (link is external) BID (link is external) CONFIRM (link is external)
graphicsmagick -- graphicsmagick	Integer underflow in the parse8BIM function in coders/meta.c in GraphicsMagick 1.3.25 and earlier allows remote attackers to cause a denial of service (application crash) via a crafted 8BIM chunk, which triggers a heap-based buffer overflow.	2017-02-06	5.0	CVE-2016-7800 SUSE SUSE DEBIAN MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
ibm -- connections	IBM Connections 5.5 and earlier allows remote attackers to obtain sensitive information by reading stack traces in returned responses.	2017-02-08	4.0	CVE-2016-0307 CONFIRM (link is external) BID (link is external)
ibm -- connections	IBM Connections 5.5 and earlier is vulnerable to possible link manipulation attack that could result in the display of inappropriate background images.	2017-02-08	4.0	CVE-2016-0308 CONFIRM (link is external) BID (link is external)
ibm -- security_key_lifecycle_manager	IBM Tivoli Key Lifecycle Manager 2.0.1, 2.5, and 2.6 generates an error message that includes sensitive information about its environment, users, or associated data.	2017-02-07	4.0	CVE-2016-6094 CONFIRM (link is external) BID (link is external)
ibm -- security_key_lifecycle_manager	IBM Tivoli Key Lifecycle Manager 2.0.1, 2.5, and 2.6 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the	2017-02-07	4.3	CVE-2016-6096 CONFIRM (link is external) BID (link is external)

	intended functionality potentially leading to credentials disclosure within a trusted session.			
libavformat_project -- libavformat	Integer overflow in the demuxer function in libmpdemux/demux_gif.c in Mplayer allows remote attackers to cause a denial of service (crash) via large dimensions in a gif file.	2017-02-03	4.3	CVE-2016-4352 MLIST (link is external) CONFIRM (link is external)
libavformat_project -- libavformat	The avcodec_decode_audio4 function in libavcodec in libavformat 57.34.103, as used in MPlayer, allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mp3 file.	2017-02-03	4.3	CVE-2016-5115 MLIST (link is external) CONFIRM (link is external)
libtiff -- libtiff	Buffer overflow in the readgifimage function in gif2tiff.c in the gif2tiff tool in LibTIFF 4.0.6 allows remote attackers to cause a denial of service (segmentation fault) via a crafted gif file.	2017-02-06	4.3	CVE-2016-5102 CONFIRM BID (link is external) CONFIRM (link is external) GENTOO
linux -- linux_kernel	include/linux/init_task.h in the Linux kernel before 2.6.35 does not prevent signals with a process group ID of zero from reaching the swapper process, which allows local users to cause a denial of service (system crash) by leveraging access to this process group.	2017-02-06	4.9	CVE-2010-5328 CONFIRM (link is external) CONFIRM CONFIRM CONFIRM MLIST (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	The smbhash function in fs/cifs/smbencrypt.c in the Linux kernel 4.9.x before 4.9.1 interacts incorrectly with the CONFIG_VMAP_STACK option, which allows local users to cause a denial of service (system crash or memory corruption) or possibly have unspecified other impact by leveraging use of more than one virtual page for a scatterlist.	2017-02-06	4.9	CVE-2016-10154 CONFIRM CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)

linux -- linux_kernel	The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.9.8 does not properly validate meta block groups, which allows physically proximate attackers to cause a denial of service (out-of-bounds read and system crash) via a crafted ext4 image.	2017-02-06	4.9	CVE-2016-10208 CONFIRM FULLDISC MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	An information disclosure vulnerability in the NVIDIA video 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-32721029. References: N-CVE-2017-0448.	2017-02-08	4.3	CVE-2017-0448 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	The load_segment_descriptor implementation in arch/x86/kvm/emulate.c in the Linux kernel before 4.9.5 improperly emulates a "MOV SS, NULL selector" instruction, which allows guest OS users to cause a denial of service (guest OS crash) or gain guest OS privileges via a crafted application.	2017-02-06	4.6	CVE-2017-2583 CONFIRM CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	The nested_vmx_check_vmptr function in arch/x86/kvm/vmx.c in the Linux kernel through 4.9.8 improperly emulates the VMXON instruction, which allows KVM L1 guest OS users to cause a denial of service (host OS memory consumption) by leveraging the mishandling of page references.	2017-02-06	4.9	CVE-2017-2596 MLIST (link is external) BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	The vc4_get_bcl function in drivers/gpu/drm/vc4/vc4_gem.c in the VideoCore DRM driver in the Linux kernel before 4.9.7 does not set an errno value upon certain overflow detections, which allows local users to cause a denial of service (incorrect pointer dereference and OOPS) via inconsistent size values in a	2017-02-06	4.9	CVE-2017-5577 CONFIRM CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external)

	VC4_SUBMIT_CL ioctl call.			CONFIRM (link is external) MLIST
netapp -- snap_creator_framework	Cross-site request forgery (CSRF) vulnerability in NetApp Snap Creator Framework before 4.3.0P1 allows remote attackers to hijack the authentication of users for requests that have unspecified impact via unknown vectors.	2017-02-07	6.8	CVE-2016-5372 CONFIRM (link is external)
openafs -- openafs	OpenAFS 1.6.19 and earlier allows remote attackers to obtain sensitive directory information via vectors involving the (1) client cache partition, (2) fileserver vice partition, or (3) certain RPC responses.	2017-02-06	5.0	CVE-2016-9772 MLIST (link is external) BID (link is external) CONFIRM
openjpeg -- openjpeg	The sycc422_t_rgb function in common/color.c in OpenJPEG before 2.1.1 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted jpeg2000 file.	2017-02-03	4.3	CVE-2016-3183 MLIST (link is external) CONFIRM (link is external) CONFIRM (link is external) CONFIRM (link is external) FEDORA FEDORA FEDORA FEDORA GENTOO
opensuse_project -- opensuse	magick/render.c in GraphicsMagick before 1.3.24 allows remote attackers to cause a denial of service (arithmetic exception and application crash) via a crafted svg file.	2017-02-03	4.3	CVE-2016-5241 SUSE SUSE CONFIRM MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
plone -- plone	Cross-site scripting (XSS) vulnerability in the manage_findResult component in the search feature in Zope ZMI in Plone before 4.3.12 and 5.x before 5.0.7 allows remote attackers to inject arbitrary web script or HTML via vectors involving double quotes, as demonstrated by the	2017-02-04	4.3	CVE-2016-7147 BID (link is external) MISC MISC MISC (link is external)

	obj_ids:tokens parameter. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-7140.			
sanadata -- sanacms	Cross-site scripting (XSS) vulnerability in index.asp in SANADATA SanaCMS 7.3 allows remote attackers to inject arbitrary web script or HTML via the search parameter.	2017-02-04	4.3	CVE-2017-5882 BID (link is external) MISC (link is external)
sendquick -- avera_sms_gateway_firmware	An issue was discovered on SendQuick Entera and Avera devices before 2HF16. An attacker could request and download the SMS logs from an unauthenticated perspective.	2017-02-05	5.0	CVE-2017-5137 BID (link is external) MISC (link is external)
sogo -- sogo	Memory leak in SOGo 2.3.7 allows remote attackers to cause a denial of service (memory consumption) via a large number of attempts to upload a large attachment, related to temporary files.	2017-02-03	6.8	CVE-2016-6188 MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
suse -- linux_enterprise_debuginfo	Multiple buffer overflows in GraphicsMagick 1.3.23 allow remote attackers to cause a denial of service (crash) via a crafted SVG file, related to the (1) TracePoint function in magick/render.c, (2) GetToken function in magick/utility.c, and (3) GetTransformTokens function in coders/svg.c.	2017-02-03	4.3	CVE-2016-2317 SUSE SUSE SUSE DEBIAN MLIST (link is external) MLIST (link is external) MLIST (link is external) MLIST (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
suse -- linux_enterprise_debuginfo	GraphicsMagick 1.3.23 allows remote attackers to cause a denial of service (NULL pointer dereference) via a crafted SVG file, related to the (1) DrawImage function in magick/render.c, (2) SVGStartElement	2017-02-03	4.3	CVE-2016-2318 SUSE SUSE SUSE DEBIAN MLIST (link is

	function in coders/svg.c, and (3) TraceArcPath function in magick/render.c.			external) MLIST (link is external) MLIST (link is external) MLIST (link is external) MLIST (link is external) BID (link is external) CONFIRM (link is external)
zoneminder -- zoneminder	Multiple reflected XSS vulnerabilities exist within form and link input parameters of ZoneMinder v1.30 and v1.29, an open-source CCTV server web application, which allows a remote attacker to execute malicious scripts within an authenticated client's browser. The URL is /zm/index.php and sample parameters could include action=login&view=postlogin[XSS] view=console[XSS] view=groups[XSS] view=events&filter[terms][1][cnj]=and[XSS] view=events&filter%5Bterms%5D%5B1%5D%5Bcnj%5D=and[XSS] view=events&filter%5Bterms%5D%5B1%5D%5Bcnj%5D=[XSS]and view=events&limit=1%22%3E%3C/a%3E[XSS] (among others).	2017-02-06	4.3	CVE-2017-5367 MISC MISC BID (link is external)
zoneminder -- zoneminder	ZoneMinder v1.30 and v1.29, an open-source CCTV server web application, is vulnerable to CSRF (Cross Site Request Forgery) which allows a remote attack to make changes to the web application as the current logged in victim. If the victim visits a malicious web page, the attacker can silently and automatically create a new admin user within the web application for remote persistence and further attacks. The URL is /zm/index.php and sample parameters could include action=user uid=0 newUser[Username]=attacker1 newUser[Password]=Password1234 conf_password=Password1234 newUser[System]=Edit (among others).	2017-02-06	6.8	CVE-2017-5368 MISC MISC BID (link is external)

Low Severity Vulnerabilities				
The Primary Vendor --- Product	**Description**	**Date Published**	**CVSS Score**	**The CVE Identity**
dotcms -- dotcms	XSS was discovered in dotCMS 3.7.0, with an authenticated attack against the /myAccount addressID parameter.	2017-02-06	3.5	CVE-2017-5875 BID (link is external) MISC (link is external)
freebsd -- freebsd	bsnmpd, as used in FreeBSD 9.3, 10.1, and 10.2, uses world-readable permissions on the snmpd.config file, which allows local users to obtain the secret key for USM authentication by reading the file.	2017-02-07	2.1	CVE-2015-5677 CONFIRM (link is external) FREEBSD
google -- android	An elevation of privilege vulnerability in Bluetooth could enable a proximate attacker to manage access to documents on the device. This issue is rated as Moderate because it first requires exploitation of a separate vulnerability in the Bluetooth stack. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32612586.	2017-02-08	2.9	CVE-2017-0423 BID (link is external) CONFIRM (link is external)
ibm -- connections	IBM Connections is vulnerable to cross-site scripting, caused by improper validation of user-supplied input. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's Web browser within the security context of the hosting Web site, once the URL is clicked. An attacker could use this vulnerability to steal the victim's cookie-based authentication credentials.	2017-02-08	3.5	CVE-2016-0305 CONFIRM (link is external) BID (link is external)
ibm -- connections	IBM Connections 5.5 and earlier is vulnerable to possible host header injection attack that could cause navigation to the attacker's domain.	2017-02-08	3.5	CVE-2016-0310 CONFIRM (link is external) BID (link is

				external)
ibm -- security_key_lifecycle_manager	IBM Tivoli Key Lifecycle Manager 2.0.1, 2.5, and 2.6 stores user credentials in plain in clear text which can be read by a local user.	2017-02-07	2.1	CVE-2016-6092 CONFIRM (link is external)
ibm -- security_key_lifecycle_manager	IBM Tivoli Key Lifecycle Manager 2.0.1, 2.5, and 2.6 allows web pages to be stored locally which can be read by another user on the system.	2017-02-07	2.1	CVE-2016-6097 CONFIRM (link is external) BID (link is external)
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm Secure Execution Environment Communicator 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-31704078. References: QC-CR#1076407.	2017-02-08	2.6	CVE-2016-8414 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	An information disclosure vulnerability in the Qualcomm sound driver could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31796345. References: QC-CR#1073129.	2017-02-08	2.6	CVE-2017-0451 BID (link is external) CONFIRM (link is external)
linux -- linux_kernel	The klsi_105_get_line_state function in drivers/usb/serial/kl5kusb105.c in the Linux kernel before 4.9.5 places uninitialized heap-memory contents into a log entry upon a failure to read the line status, which allows local users to obtain sensitive information by reading the log.	2017-02-06	2.1	CVE-2017-5549 CONFIRM CONFIRM MLIST (link is external) BID (link is external) CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	Off-by-one error in the pipe_advance function in lib/iov_iter.c in the Linux kernel before 4.9.5 allows local users to obtain sensitive information from uninitialized heap-memory locations in opportunistic circumstances by reading from a pipe	2017-02-06	2.1	CVE-2017-5550 CONFIRM CONFIRM MLIST (link is external) BID (link is external)

	after an incorrect buffer-release decision.			CONFIRM (link is external) CONFIRM (link is external)
linux -- linux_kernel	The simple_set_acl function in fs/posix_acl.c in the Linux kernel before 4.9.6 preserves the setgid bit during a setxattr call involving a tmpfs filesystem, which allows local users to gain group privileges by leveraging the existence of a setgid program with restrictions on execute permissions. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-7097.	2017-02-06	3.6	CVE-2017-5551 CONFIRM CONFIRM MLIST (link is external) BID (link is external) CONFIRM (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).