PRODUCT	DESCRIPTION	AFFECTED VERSIONS	OTHER INFORMATION
Linux Kernel 4.4.22 - 4.4.28 Remote Privilege Escalation (Root Access) via a Crafted Application	The __get_user_asm_ex macro in arch/x86/include/asm/uaccess.h in the Linux kernel 4.4.22 through 4.4.28 contains extended asm statements that are incompatible with the exception table, which allows local users to obtain root access on non-SMEP platforms via a crafted application. NOTE: this vulnerability exists because of incorrect backporting of the CVE-2016-9178 patch to older kernels.	Version(s): Linux kernel 4.4.22 through 4.4.28	Published - November 27 ,2016 CVE-2016-9644 CVSS - 9.3 Vendor's Advisory Available at : http://www.securityfocus.com/bid/94545
Linux Kernel <4.8.7 security/keys/big_key.c Remote DoS via a Crafted Application	security/keys/big_key.c in the Linux kernel before 4.8.7 mishandles unsuccessful crypto registration in conjunction with successful key-type registration, which allows local users to cause a denial of service (NULL pointer dereference and panic) or possibly have unspecified other impact via a crafted application that uses the big_key data type.	Version(s): Linux kernel before 4.8.7	Published - November 27, 2016 CVE-CVE-2016-9313 CVSS - 9.3 Vendor's Advisory Available at: http://www.securityfocus.com/bid/94546
Google Android <=7.1 Remote Privilege Escalation in Kernel Memory Subsystem	The kernel memory subsystem in Google Android 7.1 and earlier before 2016-12-05 on Pixel C, Pixel, and Pixel XL, allows remote attackers to execute arbitrary code with kernel privileges via a crafted application, aka Android internal bug 31596597. This issue is due to a use-after-free vulnerability in 'pcpu_extend_area_map()' in Linux Kernel.	Version(s): Google Android 7.1 and earlier before 2016-12-05 on Pixel C, Pixel, and Pixel XL	Published - December 05,2016 CVE-2016-4794 CVSS - 9.3 Vendor's Advisory Available at: http://www.securityfocus.com/bid/90625
Google Android <=7.1 on Nexus Devices Remote Code Execution in Qualcomm MSM Interface	Google Android 7.1 and earlier before 2016-12-05, on Nexus 6, Nexus 6P and Android One allows remote attackers to execute arbitrary code via a crafted application, aka Android internal bug 31805216. This issue exist due to a flaw in the Qualcomm MSM interface.	Version(s): Google Android 7.1 and earlier before 2016-12-05, on Nexus 6, Nexus 6P and Android One	Published - December 05,2016 CVE-2016-8411 CVSS - 8.5 The vendor's advisory is available at: https://www.vmware.com/security/advisories/VMSA-2016-0010.html
Google Android <=7.1 Remote Code Execution in the MediaTek Driver	MediaTek driver in Google Android 7.1 and earlier before 2016-12-05 allows remote attackers to execute arbitrary code via a crafted application, aka Android internal bug 31095175	Version(s): MediaTek driver in Google Android 7.1 and earlier before 2016-12-05	Published -December 05,2016 CVE-2016-6781 CVSS - 9.3 Vendor's Advisory Available at http://source.android.com/security/bulletin/2016-12-01.html
Google Android <=7.1 on Nexus Devices Remote Code Execution in Qualcomm Media Codecs	Qualcomm media codecs in Google Android 7.1 and earlier before 2016-12-05 on Nexus 5X, Nexus 6, Nexus 6P, Nexus 9, Android One, Nexus Player, Pixel and Pixel XL allows remote attackers to execute arbitrary code via a crafted application, aka Android internal bug 29421682.	Version(s): Google Android 7.1 and earlier before 2016-12-05 on Nexus 5X, Nexus 6, Nexus 6P, Nexus 9, Android One, Nexus Player, Pixel and Pixel XL	Published -December 05,2016 CVE-2016-6761 CVSS - 9.3 The vendor's advisory is available at: http://source.android.com/security/bulletin/2016-12-01.html
Google Android <=7.1 on Nexus 9 Remote Privilege Escalation in HTC Sound Codec Driver	HTC sound codec driver in Google Android 7.1 and earlier before 2016-12-05, on Nexus 9, allows remote attackers to execute arbitrary code with kernel privileges via a crafted application, aka Android internal bug 31384646. Exploitation o this issue requires the use of another vulnerability first.	Version(s): Google Android 7.1 and earlier before 2016-12-05, on Nexus 9	Published - December 05,2016 CVE-2016-6778 CVSS - 9.3 Vendor's Advisory Available at http://source.android.com/security/bulletin/2016-12-01.html
Google Android <=7.1 on Nexus Devices Remote Code Execution in the Kernel Performance Subsystem	The kernel performance subsystem in Google Android 7.1 and earlier before 2016-12-05 on Nexus 5X, Nexus 6, Nexus 6P, Nexus 9, Android One, Pixel C, Nexus Player, Pixel and Pixel XL allows remote attackers to execute arbitrary code via a crafted application, aka Android internal bug 30955111	Version(s) : Google Android 7.1 and earlier before 2016-12-05 on Nexus 5X, Nexus 6, Nexus 6P, Nexus 9, Android One, Pixel C, Nexus Player, Pixel and Pixel XL	Published - December 05, 2016 CVE-2016-6787 CVSS - 9.3 Vendor's Advisory Available at http://source.android.com/security/bulletin/2016-12-01.html
Google Android <=7.1 Remote Privilege Escalation in Broadcom Wi-Fi Driver	The Broadcom Wi-Fi driver in Google Android 7.1 and earlier before 2016-12-05, allows remote attackers to execute arbitrary code with kernel privileges via a crafted application, aka Android internal bug 31746399. Exploitation of this issue requires compromising a privileged process beforehand.	Version(s): Google Android 7.1 and earlier before 2016-12-05	Published - December 05, 2016 CVE-2014-9910 CVSS - 9.3 Vendor's Advisory Available : http://source.android.com/security/bulletin/2016-12-01.html
Google Android <=7.1 Remote Privilege Escalation in Synaptics Touchscreen Driver	The synaptics touchscreen driver in Google Android 7.1 and earlier before 2016-12-05, on Nexus 9, and Android One, allows remote attackers to execute arbitrary code with kernel privileges via a crafted application, aka Android internal bug 31913197. Exploitation of this issue requires compromising a privileged process beforehand.	Version(s): Google Android 7.1 and earlier before 2016-12-05, on Nexus 9, and Android One	Published - December 05,2016 CVE-2016-8394 CVSS - 9.3 Vendor's Advisory Available at: http://source.android.com/security/bulletin/2016-12-01.html
Google Android <=7.1 Remote Privilege Escalation in Kernel Security Subsystem	The kernel security subsystem in Google Android 7.1 and earlier before 2016-12-05, on Nexus 5X, Nexus 6, Nexus 6P, Nexus 9, Android One, Nexus Player, Pixel, and Pixel XL, allows remote attackers to execute arbitrary code with kernel privileges via a crafted application, aka Android internal bug 31253168. Exploitation of this issue requires compromising a privileged process beforehand. This issue is due to improper garbage collection in keyrings in Linux kernel.	Version(s): Google Android 7.1 and earlier before 2016-12-05, on Nexus 5X, Nexus 6, Nexus 6P, Nexus 9, Android One, Nexus Player, Pixel, and Pixel XL	Published - December 05, 2016 CVE-2015-7872 CVSS -9.3 Vendor's Advisory Available: http://source.android.com/security/bulletin/2016-12-01.html