

Histórico de vulnerabilidades de Agosto del 2016

Primary Vendor - Product	Description	Published	CVSS Score	Source & Patch Info
dbd-mysql_project - dbd-mysql	Use-after-free vulnerability in the my_login function in DBD-mysql before 4.033_01 allows attackers to have unspecified impact by leveraging a call to mysql_arma after a failure of my_login.	19/08/2016	10.0	CVE-2016-8949
fs - big_ip_access_policy_manager	The Configuration utility in FS BIG-IP LTM, Analytics, APM, ASM, GTM, and Link Controller 11.x before 11.2.1 HF16, 11.3.x, 11.4.x before 11.4.1 HF10, 11.5.x before 11.5.4, and 11.6.x before 11.6.1; BIG-IP AAM 11.x before 11.4.1 HF10, 11.5.x before 11.5.4, and 11.6.x before 11.6.1; BIG-IP ASM and PSM 11.3.x, 11.4.x before 11.4.1 HF10, 11.5.x before 11.5.4, and 11.6.x before 11.6.1; BIG-IP Edge Gateway, WebAccelerator, and WOM 11.x before 11.2.1 HF16 and 11.3.0; and BIG-IP PSM 11.x before 11.2.1 HF16, 11.3.x, and 11.4.x before 11.4.1 HF10 allows remote authenticated users with certain permissions to gain privileges by leveraging an Access Policy Manager customizations configuration section that allows file uploads.	19/08/2016	8.5	CVE-2016-8922

Semana 15/08/2016

Primary Vendor - Product	Description	Published	CVSS Score	Source & Patch Info
apple - iphone_os	iOMobileFrameBuffer in Apple iOS before 9.3.4 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	18/08/2016	9.3	CVE-2016-4654
cisco - application_policy_infrastructure_controller_enterprise_module	The Grapevine update process in Cisco Application Policy Infrastructure Controller Enterprise Module (APIC-EM) 1.0 allows remote authenticated users to execute arbitrary code as root via a crafted upgrade parameter. aka Bug ID CSCu55507	18/08/2016	8.5	CVE-2016-1165
cisco - firepower_management_center	The web-based GUI in Cisco Firepower Management Center 4.x and 5.x before 5.3.1.2 and 5.4.x before 5.4.0.1 and Cisco Adaptive Security Appliance (ASA) Software on 5500-X devices with FirePOWER Services 4.x and 5.x before 5.3.1.2 and 5.4.x before 5.4.0.1 allows remote authenticated users to execute arbitrary commands as root via crafted HTTP requests. aka Bug ID CSCv3513	18/08/2016	9.0	CVE-2016-1457
cisco - firepower_management_center	The web-based GUI in Cisco Firepower Management Center 4.x and 5.x before 5.3.0.3, 5.3.1.x before 5.3.1.2, and 5.4.x before 5.4.0.1 and Cisco Adaptive Security Appliance (ASA) Software on 5500-X devices with FirePOWER Services 4.x and 5.x before 5.3.0.3, 5.3.1.x before 5.3.1.2, and 5.4.x before 5.4.0.1 allows remote authenticated users to increase user account privileges via crafted HTTP requests. aka Bug ID CSCv25483	18/08/2016	9.0	CVE-2016-1458
cisco - adaptive_security_appliance_software	Buffer overflow in Cisco Adaptive Security Appliance (ASA) Software through 9.4.2.3 on ASA 5500, ASA 5500-X, ASA Services Module, ASA 1000V, ASAV, Firepower 9300 ASA Security Module, PIX, and FWSM devices allows remote authenticated users to execute arbitrary code via crafted IPsec SPM packets. aka Bug ID CSCv21151 or EXTKABACDN.	18/08/2016	8.5	CVE-2016-6166

Semana 08/08/2016

Primary Vendor - Product	Description	Published	CVSS Score	Source & Patch Info
haxe - libcurl	Use-after-free vulnerability in libcurl before 7.50.1 allows attackers to control which connection is used or possibly have unspecified other impact via unknown vectors.	10/08/2016	7.5	CVE-2016-5421
redhat - enterprise_linux_server	Stack-based buffer overflow in the merge_cython_line function in cacherng.cgi in the squid package before 3.1.23.16.e1c, 8.6 in Red Hat Enterprise Linux 8 allows remote attackers to execute arbitrary code via unspecified vectors. NOTE: This vulnerability exists because of an incorrect fix for CVE-2016-4901.	10/08/2016	7.5	CVE-2016-5408
microsoft - internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code via a crafted web page, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3200.	09/08/2016	7.6	CVE-2016-3288
microsoft - edge	Microsoft Internet Explorer 11 and Edge allow remote attackers to execute arbitrary code via a crafted web page, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3288.	09/08/2016	7.6	CVE-2016-3289
microsoft - internet_explorer	Microsoft Internet Explorer 11 allows remote attackers to execute arbitrary code via a crafted web page, aka "Internet Explorer Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3288.	09/08/2016	7.6	CVE-2016-3290
microsoft - edge	Microsoft Internet Explorer 9 through 11 and Edge allow remote attackers to execute arbitrary code via a crafted web page, aka "Microsoft Browser Memory Corruption Vulnerability."	09/08/2016	7.6	CVE-2016-3193
microsoft - edge	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."	09/08/2016	7.6	CVE-2016-3296
microsoft - windows_8.1	The Netlogon service in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, and Windows RT 8.1 improperly establishes secure communications channels, which allows local users to gain privileges by leveraging access to a domain-joined machine, aka "Netlogon Elevation of Privilege Vulnerability."	09/08/2016	7.2	CVE-2016-3100
microsoft - live_meeting	The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607; Office 2007 SP1, Office 2010 SP1, Word Viewer, Skype for Business 2016, Lync 2013 SP1, Lync 2010, Lync 2010 Attendee; and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Windows Graphics Component RCE Vulnerability."	09/08/2016	9.3	CVE-2016-3101
microsoft - live_meeting	The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Office 2007 SP1, Office 2010 SP1, Word Viewer, Skype for Business 2016, Lync 2013 SP1, Lync 2010, Lync 2010 Attendee; and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Windows Graphics Component RCE Vulnerability," a different vulnerability than CVE-2016-3100.	09/08/2016	9.3	CVE-2016-3103
microsoft - live_meeting	The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Office 2007 SP1, Office 2010 SP1, Word Viewer, Skype for Business 2016, Lync 2013 SP1, Lync 2010, Lync 2010 Attendee; and Live Meeting 2007 Console allows remote attackers to execute arbitrary code via a crafted embedded font, aka "Windows Graphics Component RCE Vulnerability," a different vulnerability than CVE-2016-3100.	09/08/2016	9.3	CVE-2016-3104
microsoft - windows_10	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3308, CVE-2016-3310, and CVE-2016-3311.	09/08/2016	7.2	CVE-2016-3108
microsoft - windows_10	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3308, CVE-2016-3310, and CVE-2016-3311.	09/08/2016	7.2	CVE-2016-3109
microsoft - windows_10	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3308, CVE-2016-3309, and CVE-2016-3311.	09/08/2016	7.2	CVE-2016-3110
microsoft - windows_10	The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8.1, and Windows 10 Gold, 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3308, CVE-2016-3309, and CVE-2016-3311.	09/08/2016	7.2	CVE-2016-3111
microsoft - office	Microsoft Office 2007 SP1, 2010 SP2, 2013 SP1, 2013 RT SP1, and 2016, Word 2016 for Mac, and Word Viewer allow remote attackers to execute arbitrary code via a crafted file, aka "Microsoft Office Memory Corruption Vulnerability."	09/08/2016	9.3	CVE-2016-3113
microsoft - word	Microsoft Word 2013 SP1, 2013 RT SP1, 2016, and 2016 for Mac allow remote attackers to execute arbitrary code via a crafted file, aka "Microsoft Office Memory Corruption Vulnerability."	09/08/2016	9.3	CVE-2016-3114
microsoft - office	Microsoft Office 2010 SP1, Word 2007 SP1, Word 2010 SP2, Word for Mac 2011, Word 2016 for Mac, and Word Viewer allow remote attackers to execute arbitrary code via a crafted file, aka "Microsoft Office Memory Corruption Vulnerability."	09/08/2016	9.3	CVE-2016-3117
microsoft - office	Microsoft Office 2007 SP1, 2010 SP2, 2013 SP1, and 2013 RT SP1 allow remote attackers to execute arbitrary code via a crafted file, aka "Graphics Component Memory Corruption Vulnerability."	09/08/2016	9.3	CVE-2016-3118
microsoft - edge	The PDF library in Microsoft Windows 8.1, Windows Server 2012 Gold and R2, Windows 10 Gold, 1511, and 1607; and Microsoft Edge allows remote attackers to execute arbitrary code via a crafted PDF file, aka "Microsoft PDF Remote Code Execution Vulnerability."	09/08/2016	9.4	CVE-2016-3119
microsoft - edge	Microsoft Internet Explorer 11 and Edge allow remote attackers to execute arbitrary code via a crafted web page, aka "Microsoft Browser Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3288.	09/08/2016	7.6	CVE-2016-3122
cisco - n110w_wireless_vpn_firewall_firmware	The CLI command parser on Cisco RV110W, RV130W, and RV125W devices allows local users to execute arbitrary shell commands as an administrator via crafted parameters. aka Bug IDs CSCu90134, CSCu58163, and CSCu73567.	07/08/2016	7.2	CVE-2016-6426
cisco - n110w_wireless_vpn_firewall_firmware	Cisco RV110W, RV130W, and RV125W devices have an incorrect RAC configuration for the default account, which allows remote authenticated users to obtain root access via a login session with that account. aka Bug IDs CSCu90139, CSCu58176, and CSCu73557.	07/08/2016	9.0	CVE-2016-6397
cisco - n180_vpn_router_firmware	Directory traversal vulnerability in the web interface on Cisco RV180 and RV180W devices allows remote attackers to read arbitrary files via a crafted HTTP request. aka Bug ID CSCv48051	07/08/2016	7.8	CVE-2016-1429
cisco - n180_vpn_router_firmware	Cisco RV180 and RV180W devices allow remote authenticated users to execute arbitrary commands as root via a crafted HTTP request. aka Bug ID CSCv48502	07/08/2016	9.0	CVE-2016-1430
cisco - unified_communications_manager	Cisco Unified Communications Manager (IM and Presence Service 9.1(1) SUI6, 9.1(1) SUI6, 9.1(1) SUI7, 10.5(2) SUI2, 10.5(2) SUI2a, 11.0(1) SUI1, and 11.1(1) SUI1) allows remote attackers to cause a denial of service (ipdip process restart) via crafted headers in a SIP packet. aka Bug ID CSCv49079.	07/08/2016	7.8	CVE-2016-1466
cisco - ios	Cisco IOS 15.5(3)S, 15.6(3)S2, 15.6(2)S1, and 15.6(2)T1 does not properly dequeue invalid NTP packets, which allows remote attackers to cause a denial of service (interface shutdown) by sending many crafted NTP packets. aka Bug ID CSCv39519	07/08/2016	7.8	CVE-2016-1478
google - chrome	Heap-based buffer overflow in the ogg_oh_read_SQOC_SQOC function in j2k.c in OpenJPEG, as used in POFium in Google Chrome before 52.0.2743.116, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted JPEG 2000 data.	07/08/2016	7.5	CVE-2016-5140
google - chrome	The Web Cryptography API (aka WebCrypto) implementation in Blink, as used in Google Chrome before 52.0.2743.116, does not properly copy data buffers, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted JavaScript code, related to NormalizeAlgorithm.cpp and SubtleCrypto.cpp.	07/08/2016	7.5	CVE-2016-5142
google - chrome	The Developer Tools (aka DevTools) subsystem in Blink, as used in Google Chrome before 52.0.2743.116, mishandles the script-path hostname, remoteBase parameter, and remotefontendURL parameter, which allows remote attackers to bypass intended access restrictions via a crafted URL, a different vulnerability than CVE-2016-5144.	07/08/2016	7.5	CVE-2016-5143
google - chrome	The Developer Tools (aka DevTools) subsystem in Blink, as used in Google Chrome before 52.0.2743.116, mishandles the script-path hostname, remoteBase parameter, and remotefontendURL parameter, which allows remote attackers to bypass intended access restrictions via a crafted URL, a different vulnerability than CVE-2016-5143.	07/08/2016	7.5	CVE-2016-5144
google - chrome	Multiple unspecified vulnerabilities in Google Chrome before 52.0.2743.116 allow attackers to cause a denial of service or possibly have other impact via unknown vectors.	07/08/2016	7.5	CVE-2016-5146
ibm - ipaddr_security_information_and_event_manager	IBM Security QRadar SIEM 7.1.x and 7.2.x before 7.2.7 allows remote authenticated users to execute arbitrary OS commands as root via unspecified vectors.	07/08/2016	9.0	CVE-2016-2675
linux - linux_kernel	The vfs1_proc_general function in drivers/media/video/msm/vfe/mvfe3.c in the MSM VFE31 driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, does not validate a certain id value, which allows attackers to gain privileges or cause a denial of service (memory corruption) via an application that makes a crafted ioctl call.	07/08/2016	7.2	CVE-2016-9410
linux - linux_kernel	Use-after-free vulnerability in the msm_set_crop function in drivers/media/video/msm/cameras.c in the MSM Camera driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to gain privileges or cause a denial of service (memory corruption) via an application that makes a crafted ioctl call.	07/08/2016	7.2	CVE-2015-0569
linux - linux_kernel	drivers/media/platform/msm/brnaccad.c in the TSC driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service (invalid pointer dereference) or possibly have unspecified other impact via a crafted application that makes a TSC_CARD_STATUS ioctl call.	07/08/2016	10.0	CVE-2015-0573
linux - linux_kernel	Stack-based buffer overflow in the supply_img_input_write function in drivers/thermal/supply_img_core.c in the MSM Thermal driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service or possibly have unspecified other impact via a crafted application that sends a large amount of data through the debugfs interface.	07/08/2016	10.0	CVE-2016-2063
linux - linux_kernel	fs/proc/mounts/igmpw/mount_effects-qb-v2.c in the MSM QDSP5 audio driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted application that makes an ioctl call specifying many commands.	07/08/2016	7.2	CVE-2016-2064
linux - linux_kernel	sound/ocssm/igmpw/mount_effects-qb-v2.c in the MSM QDSP5 audio driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allows attackers to cause a denial of service (out-of-bounds write and memory corruption) or possibly have unspecified other impact via a crafted application that makes an ioctl call ingesting incorrect use of a parameters register.	07/08/2016	10.0	CVE-2016-2065
linux - linux_kernel	The is_ashmem_file function in drivers/staging/android/ashmem.c in a certain Qualcomm Innovation Center (QuIC) Android patch for the Linux kernel 3.x mishandles pointer validation within the KGS_Linux_Graphics_Module, which allows attackers to bypass intended access restrictions by using the /ashmem/area as the destination.	07/08/2016	7.2	CVE-2016-5140
mosa - softcam	SQL injection vulnerability in Mosa SoftCamS before 1.5 allows remote attackers to execute arbitrary SQL commands via unspecified fields.	07/08/2016	7.5	CVE-2016-6292

Histórico de vulnerabilidades de Agosto del 2016

Primeira Vendor / Product	Description	Published	CVSS Score	Source & Patch Info
openssh - openssh	The <code>auth_password</code> function in <code>auth-passwd.c</code> in <code>sshd</code> in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (excess CPU consumption) via a long string.	07/08/2016	7.8	CVE-2016-6515
php - php	Multiple integer overflows in <code>php_zip.c</code> in the <code>zip</code> extension in PHP before 7.0.6 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted call to (1) <code>perfrombinhex</code> or (2) <code>getFromName</code> in the <code>ZipArchive</code> class.	07/08/2016	7.5	CVE-2016-3078
php - php	Double free vulnerability in the <code>php_zip</code> extension's <code>offset</code> function in <code>ext/zip/zip_dlist.c</code> in PHP 7.x before 7.0.6 allows remote attackers to execute arbitrary code via a crafted index.	07/08/2016	7.5	CVE-2016-3132
php - php	The <code>get_tcu_value</code> internal function in <code>ext/intl/locale/locale_methods.c</code> in PHP before 5.5.36, 5.6.x before 5.6.22, and 7.x before 7.0.7 does not ensure the presence of a '0' character, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a crafted <code>scale_get_primary_language</code> call.	07/08/2016	7.5	CVE-2016-5093
php - php	Integer overflow in the <code>php_html_entities</code> function in <code>ext/standard/html.c</code> in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a large output string from a <code>FILTER_SANITIZE_FULL_SPECIAL_CHARS</code> filter. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-5094 .	07/08/2016	7.5	CVE-2016-5094
php - php	Integer overflow in the <code>head</code> function in <code>ext/standard/html.c</code> in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact by triggering a large output string from a <code>FILTER_SANITIZE_FULL_SPECIAL_CHARS</code> filter. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-5094 .	07/08/2016	7.5	CVE-2016-5095
php - php	Integer overflow in the <code>head</code> function in <code>ext/standard/html.c</code> in PHP before 5.5.36 and 5.6.x before 5.6.22 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted exception.	07/08/2016	7.5	CVE-2016-5096
php - php	Double free vulnerability in the <code>php_mib_reg_replace_exec</code> function in <code>php_mibreg.c</code> in the <code>mbstring</code> extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to execute arbitrary code or cause a denial of service (application crash) by leveraging a callback exception.	07/08/2016	7.5	CVE-2016-5108
php - php	Multiple integer overflows in <code>mysql.c</code> in the <code>mysql</code> extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allow remote attackers to cause a denial of service (heap-based buffer overflow and application crash) or possibly have unspecified other impact via a crafted length value, related to the (1) <code>mysql_generic</code> and (2) <code>mysql_generic</code> functions.	07/08/2016	7.5	CVE-2016-5109
php - php	Integer overflow in the <code>SPkiObject::read</code> function in <code>spl_directory.c</code> in the <code>SPL</code> extension in PHP before 5.5.37 and 5.6.x before 5.6.23 allows remote attackers to cause a denial of service or possibly have unspecified other impact via a large integer argument. a related issue in CVE-2016-5096	07/08/2016	7.5	CVE-2016-5170
php - php	Double free vulnerability in the <code>php_wddx_process_data</code> function in <code>wddx.c</code> in the <code>WDDX</code> extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted <code>data</code> .	07/08/2016	7.5	CVE-2016-5172
php - php	Integer overflow in the <code>php_wddx_process_data</code> function in <code>wddx.c</code> in the <code>WDDX</code> extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 allows remote attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a crafted <code>data</code> .	07/08/2016	7.5	CVE-2016-5173
siemens - sinema_server	Siemens SINEMA Server uses weak permissions for the application folder, which allows local users to gain privileges via <code>sudo</code> filed <code>setenv</code> .	07/08/2016	7.2	CVE-2016-6486
google - android	Integer underflow in the <code>diag</code> driver in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices allows attackers to gain privileges or obtain sensitive information via a crafted application. aka Android internal bug 28768146 and Qualcomm internal bug CR564761 .	06/08/2016	9.3	CVE-2016-9863
google - android	<code>drivers/misc/qpcom.c</code> in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not validate ioctl calls, which allows attackers to gain privileges via a crafted application. aka Android internal bug 28747998 and Qualcomm internal bug CR564841 .	06/08/2016	9.3	CVE-2016-9864
google - android	<code>drivers/misc/qpcom.c</code> in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not properly restrict user-space input, which allows attackers to gain privileges via a crafted application. aka Android internal bug 28748271 and Qualcomm internal bug CR565031 .	06/08/2016	9.3	CVE-2016-9865
google - android	<code>drivers/media/platform/msm/camera_v2/sensor/oid/mem_csid.c</code> in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not validate a certain parameter, which allows attackers to gain privileges via a crafted application. aka Android internal bug 28749284 and Qualcomm internal bug CR513158 .	06/08/2016	9.3	CVE-2016-9866
google - android	<code>drivers/media/platform/msm/camera_v2/sensor/mem_csid.c</code> in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not validate the number of streams, which allows attackers to gain privileges via a crafted application. aka Android internal bug 28749629 and Qualcomm internal bug CR514702 .	06/08/2016	9.3	CVE-2016-9867
google - android	<code>drivers/media/platform/msm/camera_v2/sensor/mem_csid.c</code> in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not validate certain index values, which allows attackers to gain privileges via a crafted application. aka Android internal bug 28749728 and Qualcomm internal bug CR514713 .	06/08/2016	9.3	CVE-2016-9869
google - android	The Linux kernel before 4.13 on Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not properly consider user-space access to the <code>TPIDRUW</code> register, which allows local users to gain privileges via a crafted application. aka Android internal bug 28749743 and Qualcomm internal bug CR510464 .	06/08/2016	9.3	CVE-2016-9870
google - android	Multiple buffer overflows in <code>drivers/media/platform/mem_csid.c</code> in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices allow attackers to gain privileges via a crafted application. aka Android internal bug 28749803 and Qualcomm internal bug CR514717 .	06/08/2016	9.3	CVE-2016-9871
google - android	<code>drivers/misc/qpcom.c</code> in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices does not validate certain length values, which allows attackers to gain privileges via a crafted application. aka Android internal bug 28804057 and Qualcomm internal bug CR636633 .	06/08/2016	9.3	CVE-2016-9887
google - android	Off-by-one error in <code>drivers/media/platform/mem_csid.c</code> in the Qualcomm components in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices allows attackers to gain privileges via a crafted application that sends an I2C command. aka Android internal bug 28772007 and Qualcomm internal bug CR529177 .	06/08/2016	9.3	CVE-2016-9890
google - android	<code>drivers/misc/qpcom.c</code> in the Qualcomm components in Android before 2016-08-05 on Nexus 5 devices does not validate certain buffer addresses, which allows attackers to gain privileges via a crafted application that makes an ioctl call. aka Android internal bug 28749283 and Qualcomm internal bug CR550061 .	06/08/2016	9.3	CVE-2016-9838
google - android	The MSM camera driver in the Qualcomm components in Android before 2016-08-05 on Nexus 5 devices does not validate input parameters, which allows attackers to gain privileges via a crafted application. aka Android internal bug 28804030 and Qualcomm internal bug CR766022 .	06/08/2016	9.3	CVE-2016-9839
google - android	<code>drivers/video/mem/mem_csid.c</code> in the Qualcomm components in Android before 2016-08-05 on Nexus 7 (2013) devices does not validate <code>g_stages</code> , <code>g_stages</code> , or <code>h_stages</code> data, which allows attackers to gain privileges via a crafted application. aka Android internal bug 28398884 and Qualcomm internal bug CR779011 .	06/08/2016	9.3	CVE-2016-9840
google - android	Integer overflow in <code>sound/sof/igmp2/igmp2.c</code> in the Qualcomm components in Android before 2016-08-05 on Nexus 6 devices allows attackers to gain privileges via a crafted application. aka Android internal bug 28823987 and Qualcomm internal bug CR792367 .	06/08/2016	9.3	CVE-2016-9840
google - android	<code>drivers/media/platform/mem_csid.c</code> in the Qualcomm components in Android before 2016-08-05 on Nexus 6 and 7 (2013) devices does not properly validate array indexes, which allows attackers to gain privileges via a crafted application. aka Android internal bug 28814509 and Qualcomm internal bug CR792473 .	06/08/2016	9.3	CVE-2016-9841
google - android	<code>drivers/media/platform/mem_csid.c</code> in the Qualcomm components in Android before 2016-08-05 on Nexus 6 devices does not validate the stream state, which allows attackers to gain privileges via a crafted application. aka Android internal bug 28814602 and Qualcomm internal bug CR803246 .	06/08/2016	9.3	CVE-2016-9842
google - android	The IPv6 stack in the Linux kernel before 4.3.3 mishandles options data, which allows local users to gain privileges or cause a denial of service (user-space access and system crash) via a crafted <code>sendmsg</code> system call.	06/08/2016	7.2	CVE-2016-3841
linux - linux_kernel	<code>pci/arc/mem/dma-mapping.c</code> in the Linux kernel before 4.13 on ARM platforms, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not prevent executable DMA mappings, which might allow local users to gain privileges via a crafted application. aka Android internal bug 28828142 and Qualcomm internal bug CR642735 .	06/08/2016	7.2	CVE-2016-9888
linux - linux_kernel	The <code>aggregator</code> <code>setprocattr</code> function in <code>security/apparmor.c</code> in the Linux kernel before 4.6.5 does not validate the buffer size, which allows local users to gain privileges by triggering an <code>AppArmor</code> <code>setprocattr</code> hook.	06/08/2016	7.2	CVE-2016-6187
dashbuilder_project - dashbuilder	SQL injection vulnerability in the <code>getServiceParametersSQL</code> method in <code>main/java/org/dashbuilder/datasource/impl/dialect/DefaultDialect.java</code> in Dashbuilder before 0.6.0 Beta1 allows remote attackers to execute arbitrary SQL commands via a <code>data</code> set lookup filter in the (1) <code>Data Set Autoring</code> or (2) <code>Designer</code> editor UI.	05/08/2016	7.5	CVE-2016-4999
google - android	The Qualcomm Wi-Fi driver in Android before 2016-08-05 on Nexus 7 (2013) devices makes incorrect <code>ioctl</code> calls, which allows remote attackers to cause a denial of service (device hang or reboot) via crafted frames. aka Android internal bug 28670333 and Qualcomm internal bug CR548711 .	05/08/2016	7.8	CVE-2016-9901
google - android	Buffer overflow in <code>CHRWYS/Reggy/str/utf8/str/dot11.c</code> in the Qualcomm Wi-Fi driver in Android before 2016-08-05 on Nexus 7 (2013) devices allows remote attackers to execute arbitrary code via a crafted information element (IE) in an 802.11 management frame. aka Android internal bug 28668638 and Qualcomm internal bug CR553937 and CR553941 .	05/08/2016	10.0	CVE-2016-9902
google - android	<code>services/core/java/com/android/server/pm/PackageManagerService.java</code> in the framework APIs in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-08-01 allows attackers to increase intent-filter priority via a crafted application. aka internal bug 28450495 .	05/08/2016	7.5	CVE-2016-2497
google - android	Integer overflow in <code>codes/02/h264dec/source/h264sd_0pb.c</code> in <code>libstagefright</code> in <code>media-server</code> in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-08-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file. aka internal bug 28349266 .	05/08/2016	7.5	CVE-2016-3819
google - android	The <code>h264sd</code> decoder in <code>media-server</code> in Android 4.x before 2016-08-01 mishandles slice numbers, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file. aka internal bug 28673430 .	05/08/2016	7.5	CVE-2016-3820
google - android	<code>h264sd</code> in <code>media-server</code> in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-08-01 causes incorrect declarations, which allows remote attackers to execute arbitrary code or cause a denial of service (NULL pointer dereference or memory corruption) via a crafted media file. aka internal bug 28160156 .	05/08/2016	7.5	CVE-2016-3821
google - android	<code>safe.c</code> in <code>Mathias Winder/Jsaid 2.0.7</code> , as used in <code>libstagefright</code> in <code>media-server</code> in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-08-01, allows remote attackers to execute arbitrary code or cause a denial of service (out-of-bounds access) via a crafted <code>EXIF</code> data. aka internal bug 28968315 .	05/08/2016	7.5	CVE-2016-3822
google - android	<code>codes/h264dec/02/h264dec.c</code> in <code>libstagefright</code> in <code>media-server</code> in Android 6.0.1 before 2016-08-01 mishandles decoder errors, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file. aka internal bug 28816956 .	05/08/2016	7.1	CVE-2016-3827
google - android	decoder/h264d_0pb.c in <code>media-server</code> in Android 6.x before 2016-08-01 mishandles invalid PPS and SPS NAL units, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file. aka internal bug 28835995 .	05/08/2016	7.1	CVE-2016-3828
google - android	The <code>h264sd</code> decoder in <code>media-server</code> in Android 6.x before 2016-08-01 does not initialize certain structure members, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file. aka internal bug 28023649 .	05/08/2016	7.1	CVE-2016-3829
google - android	<code>codes/h264dec/02/h264dec.c</code> in <code>libstagefright</code> in <code>media-server</code> in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-08-01 allows remote attackers to cause a denial of service (device hang or reboot) via crafted ADTS data. aka internal bug 29153099 .	05/08/2016	7.1	CVE-2016-3830
google - android	The framework APIs in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-08-01 do not ensure that package data originated from the <code>PackageManager</code> , which allows attackers to bypass an unspecified protection mechanism via a crafted application. aka internal bug 28795098 .	05/08/2016	8.1	CVE-2016-3832
google - android	The <code>Shell</code> components in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-08-01 does not properly manage the <code>MANAGE_USERS</code> and <code>CREATE_USERS</code> permissions, which allows attackers to bypass intended access restrictions via a crafted application. aka internal bug 29189712 .	05/08/2016	9.3	CVE-2016-3833
google - android	<code>Concept</code> in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-08-05 does not properly identify session reuse, which allows remote attackers to execute arbitrary code via unspecified vectors. aka internal bug 28751153 .	05/08/2016	10.0	CVE-2016-3840
google - android	The Qualcomm GPU driver in Android before 2016-08-05 on Nexus 5X, 6, and 6P devices allows attackers to gain privileges via a crafted application. aka Android internal bug 28577652 and Qualcomm internal bug CR100294 .	05/08/2016	9.3	CVE-2016-3842
google - android	Android before 2016-08-05 does not properly restrict code execution in a kernel context, which allows attackers to gain privileges via a crafted application, as demonstrated by the kernel performance subsystem and the Qualcomm performance component. aka Android internal bug 28986278 and 29139807 and Qualcomm internal bug CR1011071 .	05/08/2016	9.3	CVE-2016-3843
google - android	<code>media-server</code> in Android before 2016-08-05 on Nexus 9 and Pixel C devices allows attackers to gain privileges via a crafted application. aka internal bug 28296517 .	05/08/2016	9.3	CVE-2016-3844
google - android	The video driver in the kernel in Android before 2016-08-05 on Nexus 5 devices allows attackers to gain privileges via a crafted application. aka internal bug 28399876 .	05/08/2016	9.3	CVE-2016-3845
google - android	The Serial Peripheral Interface driver in Android before 2016-08-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application. aka internal bug 28817178 .	05/08/2016	7.6	CVE-2016-3846
google - android	The NVIDIA media driver in Android before 2016-08-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application. aka internal bug 28919417 .	05/08/2016	7.6	CVE-2016-3848

Historico de vulnerabilidades de Agosto del 2016

Primary Vendor / Product	Description	Published	CVSS Score	Source & Patch Info
google -- android	The LG Electronics bootloader Android before 2016-08-05 on Nexus 5X devices allows attackers to gain privileges by leveraging access to a privileged process, aka Internal Bug 29189941.	05/08/2016	9.8	CVE-2016-3831
google -- android	The kernel in Android before 2016-08-05 on Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Internal Bug 29227519.	05/08/2016	9.3	CVE-2016-3857
juniper -- junos	Juniper Junos OS before 12.1X46-D05, 12.1X47 before 12.1X47-D03, 12.1X48 before 12.1X48-D05, and 15.1X49 before 15.1X49-D40 on a High-End SRX Series chassis system with one or more Application Layer Gateways (ALGs) enabled allow remote attackers to cause a denial of service (CPU consumption, fab link failure, or flap-flop failures) via vectors related to in-transit traffic matching ALG rules.	05/08/2016	7.1	CVE-2016-1276
sap -- hana	The multi-tenant database container feature in SAP HANA does not properly encrypt communications, which allows remote attackers to bypass intended access restrictions and possibly have unspecified other impact via unknown vectors, aka SAP Security Note 2219350.	05/08/2016	7.5	CVE-2016-6150

Semana 01/08/2016

Primary Vendor / Product	Description	Published	CVSS Score	Source & Patch Info
sap -- trex	Directory traversal vulnerability in SAP TREX 7.10 Revision 63 allows remote attackers to read arbitrary files via unspecified vectors, aka SAP Security Note 2203591.	05/08/2016	10.0	CVE-2016-6138
sap -- trex	SAP TREX 7.10 Revision 63 allows remote attackers to read arbitrary files via unspecified vectors, aka SAP Security Note 2203591.	05/08/2016	7.6	CVE-2016-6139
sap -- trex	SAP TREX 7.10 Revision 63 allows remote attackers to write to arbitrary files via vectors related to RFC-Gateway, aka SAP Security Note 2203591.	05/08/2016	7.6	CVE-2016-6140
sap -- trex	An unspecified interface in SAP TREX 7.10 Revision 63 allows remote attackers to execute arbitrary OS commands with SIDadm privileges via unspecified vectors, aka SAP Security Note 2214276.	05/08/2016	10.0	CVE-2016-6147
mozilla -- firefox	Use-after-free vulnerability in the nsXULPopupManager::KeyDown function in Mozilla Firefox before 48.0 and Firefox ESR 45.x before 45.1 allows attackers to execute arbitrary code or cause a denial of service (heap memory corruption and application crash) by leveraging keyboard access to use the Alt key during selection of top-level menu items.	04/08/2016	7.5	CVE-2016-5214
mozilla -- firefox	Integer overflow in the WebSocketChannel class in the WebSockets subsystem in Mozilla Firefox before 48.0 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted packets that trigger incorrect buffer resize operations during buffering.	04/08/2016	7.5	CVE-2016-5261
atlassian -- bamboo	Atlassian Bamboo before 5.11.4.1 and 5.11.2 before 5.11.2.1 does not properly restrict permitted deserialized classes, which allows remote attackers to execute arbitrary code via vectors related to XStream serialization.	02/08/2016	7.5	CVE-2016-5429
citrix -- netserver	The PV pageable code in arch/ARM/mem.c in Xen 4.7.4 and earlier allows local 32-bit PV guest OS administrators to gain host OS privileges by leveraging host writes for updating pageable entries.	02/08/2016	7.2	CVE-2016-6258
crestron -- airmedia_am-100_firmware	Directory traversal vulnerability in csp_bin/flash.cgi on Crestron AirMedia AM-100 devices with firmware before 1.4.0.13 allows remote attackers to execute arbitrary commands via a .(dot dot) in the ATE_COMMAND parameter.	02/08/2016	10.0	CVE-2016-5640
crestron -- dm-txv-100-str_firmware	Crestron Electronics DM-TXV-100-STR devices with firmware before 1.3039.00040 allow remote attackers to bypass authentication via a direct request to a page other than index.html.	02/08/2016	7.5	CVE-2016-5667
crestron -- dm-txv-100-str_firmware	Crestron Electronics DM-TXV-100-STR devices with firmware before 1.3039.00040 allow remote attackers to bypass authentication and change settings via a JSON API call.	02/08/2016	7.5	CVE-2016-5668
crestron -- dm-txv-100-str_firmware	Crestron Electronics DM-TXV-100-STR devices with firmware before 1.3039.00040 have a hardcoded password of admin for the admin account, which makes it easier for remote attackers to obtain access via the web management interface.	02/08/2016	10.0	CVE-2016-5670
huawei -- cloudengine_12800_firmware	Huawei NE40E and CS200 devices with software before V800R0075P017; P7N 6802-3-488 devices with software before V800R0075P019; NS500E devices with software before V100R0055PHD18; and CloudEngine devices 12800 with software before V100R0055PHD10 and V100R0055 before V100R0055PHD06 allow remote attackers with control plane access to cause a denial of service or execute arbitrary code via a crafted packet.	02/08/2016	7.5	CVE-2016-6179
huawei -- p8_smartphone_firmware	Buffer overflow in the Wi-Fi driver in Huawei P8 smartphones with software before GRA-CUC0202963 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, a different vulnerability than CVE-2016-6193.	02/08/2016	9.3	CVE-2016-6192
huawei -- p8_smartphone_firmware	Buffer overflow in the Wi-Fi driver in Huawei P8 smartphones with software before GRA-CUC0202963 allows attackers to cause a denial of service (system crash) or gain privileges via a crafted application, a different vulnerability than CVE-2016-6192.	02/08/2016	9.3	CVE-2016-6193
novell -- filr	Novell Filr 1.2 before Hot Patch 6 and 2.0 before Hot Patch 2 uses world-writable permissions for /etc/profile.d/vaimit.sh, which allows local users to gain privileges by replacing this file's content with arbitrary shell commands.	31/07/2016	7.2	CVE-2016-1611
paloaltonetworks -- pan-os	Palo Alto Networks PAN-OS before 5.0.19, 5.1.x before 5.1.12, 6.0.x before 6.0.14, 6.1.x before 6.1.12, and 7.0.x before 7.0.8 might allow local users to gain privileges by leveraging improper sanitization of the root_reboot local invocation.	02/08/2016	7.2	CVE-2016-1712
perl -- perl	(1) cpan/Archive-Tar/bin/ptar, (2) cpan/Archive-Tar/bin/ptardiff, (3) cpan/Archive-Tar/bin/ptarargs, (4) cpan/CPAN/cntrpt/cpan, (5) cpan/Encode/bin/enc2hex, (6) cpan/Encode/bin/enc2hex, (7) cpan/Encode/bin/enc2hex, (8) cpan/Encode/bin/picocom, (9) cpan/Encode/bin/jumplist, (10) cpan/Encode/bin/unidump, (11) cpan/ExtUtils-MakeMaker/bin/instrmodsh, (12) cpan/IO-Compress/bin/gzipcat, (13) cpan/IO/bin/iosp, (14) cpan/Perl-Harpoon/bin/parv, (15) dist/ExtUtils-Paradox/bin/ExtUtils/Kubpp, (16) dist/Module-CoreList/corelist, (17) ext/Pod-Html/bin/pod2html, (18) util/c2ph.pl, (19) util/h2ph.pl, (20) util/h2xs.pl, (21) util/libnetcfg.pl, (22) util/perlbug.pl, (23) util/periodic.pl, (24) util/perlwp.pl, and (25) util/cpan.pl in Perl 5.x before 5.22.3-RC2 and 5.24 before 5.24.1-RC2 do not properly remove .(period) characters from the end of the includes directory array, which might allow local users to gain privileges via a Trojan horse module under the current working directory.	02/08/2016	7.2	CVE-2016-1238
pillsecure -- odyssey_access_client	An unspecified client-side component in Pulse Secure Desktop Client before 5.0-15.1, 5.1x before 5.1x-1 and 5.2x before 5.2x-1, Installer Service (formerly Juniper Installer Service) and Collaboration (formerly Secure Meeting) before 8.0-15.1, 8.1x before 8.1x-1, and 8.2x before 8.2x-1, and Odyssey Access Client before 5.6r18 on Windows allows local users to gain administrative privileges via unknown vectors.	02/08/2016	7.2	CVE-2016-2409
redhat -- jboss_operations_network	The server in Red Hat JBoss Operations Network (JON) before 3.6 allows remote attackers to execute arbitrary code via a crafted HTTP request, related to message deserialization.	02/08/2016	9.0	CVE-2016-1727
ec-cube -- coupon_plugin	SQL injection vulnerability in the Seed Coupon plugin before 1.6 for EC-CUBE allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	31/07/2016	7.5	CVE-2016-4837
hp -- operations_manager	The AdminUI in HPE Operations Manager (OM) before 9.21.130 on Linux, Unix, and Solaris allows remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.	31/07/2016	7.5	CVE-2016-4372
novell -- filr	vacan@filr in Novell Filr before 1.2 Security Update 3 and 2.0 before Security Update 2 allows remote authenticated users to execute arbitrary commands via shell metacharacters in the viteServer parameter.	31/07/2016	9.0	CVE-2016-1608