

Histórico de vulnerabilidades de Julio del 2016

Semana 25/07/2016				
Primary Vendor - Product	Description	Published	CVSS Score	Source & Patch Info
csso - unified_computing_system_performance_manager	The web framework in Cisco Unified Computing System (UCS) Performance Manager 2.0.0 and earlier allows remote authenticated users to execute arbitrary commands via crafted parameters in a GET request, aka Bug-ID CSCu07927.	27/07/2016	9.0	CVE-2016-1174
rockwellautomation - factorytalk_energymetrics	SQL injection vulnerability in Rockwell Automation FactoryTalk EnergyMetric before 2.20.00 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	27/07/2016	7.5	CVE-2016-6322
rockwellautomation - factorytalk_energymetrics	Rockwell Automation FactoryTalk EnergyMetric before 2.20.00 does not invalidate credentials upon a logout action, which makes a path for remote attackers to obtain access by leveraging an unauthenticated workstation.	27/07/2016	7.5	CVE-2016-6311
ca - ehealth	CA eHealth 6.2.x allows remote authenticated users to cause a denial of service or possibly execute arbitrary commands via unspecified vectors.	25/07/2016	9.0	CVE-2016-6131
ca - ehealth	CA eHealth 6.2 and 6.3.x before 6.3.2.13 allows remote authenticated users to cause a denial of service or possibly execute arbitrary commands via unspecified vectors.	25/07/2016	9.0	CVE-2016-6152
icu_project - international_components_for_unicode	The <code>uio_acceptLanguageFromHTTP</code> function in <code>common/uio.cpp</code> in International Components for Unicode (ICU) through 57.1 for C/C++ does not ensure that there is a '\0' character at the end of a certain temporary array, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long <code>httpAcceptLanguage</code> argument.	25/07/2016	7.5	CVE-2016-6293
php - php	The <code>php_url_parse_ex</code> function in <code>ext/standard/url.c</code> in PHP before 5.5.38 allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via vectors involving the <code>smart_str</code> data type.	25/07/2016	7.5	CVE-2016-6289
php - php	<code>ext/session/session.c</code> in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly maintain a certain hash data structure, which allows remote attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact via vectors related to session deserialization.	25/07/2016	7.5	CVE-2016-6290
php - php	The <code>ext_process_jfp_in_MAARNDOTE</code> function in <code>ext/ini/eval.c</code> in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 allows remote attackers to cause a denial of service (out-of-bounds array access and memory corruption), obtain sensitive information from process memory, or possibly have unspecified other impact via a crafted JPEG image.	25/07/2016	7.5	CVE-2016-6291
php - php	The <code>local_accept_from_http</code> function in <code>ext/intl/locale/locale_methods.c</code> in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 does not properly restrict calls to the ICU <code>uio_acceptLanguageFromHTTP</code> function, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long argument.	25/07/2016	7.5	CVE-2016-6296
php - php	<code>ext/openssl/openssl.c</code> in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9 improperly interacts with the unserialized implementation and garbage collection, which allows remote attackers to cause a denial of service (use-after-free and application crash) or possibly have unspecified other impact via crafted serialized data, a related issue to CVE-2016-5773.	25/07/2016	7.5	CVE-2016-6295
php - php	Integer signedness error in the <code>simplestring_addln</code> function in <code>simplestring.c</code> in <code>ext/openssl</code> through 0.54.2, as used in PHP before 5.5.38, 5.6.x before 5.6.24, and 7.x before 7.0.9, allows remote attackers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact via a long first argument to the <code>PHP openssl_encode_request</code> function.	25/07/2016	7.5	CVE-2016-6296
google - chrome	The PPAIR implementation in Google Chrome before 52.0.2743.82 does not validate the origin of IPC messages to the plugin broker process that should have come from the browser process, which allows remote attackers to bypass a sandbox protection mechanism via an unexpected message type, related to broker <code>_process_dispatcher.cc</code> , <code>ppapi_plugin_process_host.cc</code> , <code>ppapi_thread.cc</code> , and <code>renderer_frame_message_filter.cc</code> .	23/07/2016	9.1	CVE-2016-1106
siemens - simatic_batch	Siemens SIMATIC WinCC before 7.1 Update 7.4 before Update 1, SIMATIC BATCH before 8.1 SP1 Update 9 as distributed in SIMATIC PCS 7 through 8.1 SP1, SIMATIC OpenPCS 7 before 8.1 SP1, SIMATIC OpenPCS 7 through 8.1 SP1, SIMATIC PCS 7 before 8.2 Update 1 as distributed in SIMATIC PCS 7 8.2, and SIMATIC WinCC Runtime Professional before 11 SP1 Update 9 allow remote attackers to execute arbitrary code via crafted packets.	22/07/2016	10.0	CVE-2016-5149

Semana 18/07/2016				
Primary Vendor - Product	Description	Published	CVSS Score	Source & Patch Info
oracle - retail_integration_bus	Unspecified vulnerability in the Oracle Retail Integration Bus component in Oracle Retail Applications 13.0, 13.1, 13.2, 14.0, 14.1, and 15.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to install.	21/07/2016	10.0	CVE-2016-3444
oracle - business_intelligence	Unspecified vulnerability in the Oracle Business Intelligence Enterprise Edition component in Oracle Fusion Middleware 11.1.1.7.0 and 11.1.1.3.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Analytics Web Administration.	21/07/2016	7.5	CVE-2016-3446
oracle - agile_engineering_data_management	Unspecified vulnerability in the Oracle Agile Engineering Data Management component in Oracle Supply Chain Products Suite 6.1.3.0 and 6.2.0.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to install.	21/07/2016	10.0	CVE-2016-3449
oracle - transportation_management	Unspecified vulnerability in the Oracle Transportation Management component in Oracle Supply Chain Products Suite 6.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to install.	21/07/2016	7.5	CVE-2016-3430
oracle - mysql	Unspecified vulnerability in Oracle MySQL 5.5-5.6 and earlier and 5.6.26 and earlier allows local users to affect confidentiality, integrity, and availability via vectors related to <code>Server - Option</code> .	21/07/2016	7.5	CVE-2016-3471
oracle - mysql	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier allows local users to affect confidentiality, integrity, and availability via vectors related to <code>Server - Parser</code> .	21/07/2016	7.5	CVE-2016-3477
oracle - database	Unspecified vulnerability in the Oracle Database component in Oracle Database Server 11.2.0.4 and 12.1.0.2 allows remote attackers to affect availability via unknown vectors.	21/07/2016	7.8	CVE-2016-3479
oracle - webcenter_sites	Unspecified vulnerability in the Oracle WebCenter Sites component in Oracle Fusion Middleware 11.1.1.8, and 12.2.1.0 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	21/07/2016	10.0	CVE-2016-3487
oracle - database	Unspecified vulnerability in the Data Pump Import component in Oracle Database Server 11.2.0.4, 12.1.0.1, and 12.1.0.2 allows local users to affect confidentiality, integrity, and availability via unknown vectors.	21/07/2016	7.5	CVE-2016-3489
oracle - crm_technical_foundation	Unspecified vulnerability in the Oracle CRM Technical Foundation component in Oracle E-Business Suite 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to <code>Wireless Framework</code> .	21/07/2016	8.5	CVE-2016-3491
oracle - hyperion_financial_reporting	Unspecified vulnerability in the Hyperion Financial Reporting component in Oracle Hyperion 11.2.4 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Security Models.	21/07/2016	10.0	CVE-2016-3493
oracle - weblogic_server	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 12.1.3.0 and 12.2.1.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Web Container.	21/07/2016	10.0	CVE-2016-3499
oracle - weblogic_server	Unspecified vulnerability in the Oracle WebLogic Server component in Oracle Fusion Middleware 10.3.6.0, 12.1.3.0, and 12.2.1.0 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to WLS Core Components, a different vulnerability than CVE-2016-3586.	21/07/2016	10.0	CVE-2016-3510
oracle - customer_interaction_history	Unspecified vulnerability in the Oracle Customer Interaction History component in Oracle E-Business Suite 12.1.1, 12.1.2, and 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to Function Security.	21/07/2016	7.8	CVE-2016-3511
oracle - enterprise_communications_broker	Unspecified vulnerability in the Oracle Enterprise Communications Broker component in Oracle Communications Applications before PCS 3.0 allows remote attackers to affect confidentiality and integrity via vectors related to <code>Web Services</code> .	21/07/2016	7.5	CVE-2016-3515
oracle - web_applications_desktop_integrator	Unspecified vulnerability in the Oracle Web Applications Desktop Integrator component in Oracle E-Business Suite 12.1.3, 12.2.1, 12.2.4, and 12.2.5 allows remote attackers to affect confidentiality and integrity via vectors related to Application Service.	21/07/2016	8.5	CVE-2016-3522
oracle - agile_product_lifecycle_management_fra_integrator	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote attackers to affect confidentiality via vectors related to SDK, a different vulnerability than CVE-2016-3529 and CVE-2016-3550.	21/07/2016	7.8	CVE-2016-3526
oracle - agile_product_lifecycle_management_fra_integrator	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote authenticated users to affect integrity and availability via vectors related to <code>PCS / Import</code> .	21/07/2016	7.5	CVE-2016-3530
oracle - advanced_inbound_telephony	Unspecified vulnerability in the Oracle Advanced Inbound Telephony component in Oracle E-Business Suite 12.1.1, 12.1.2, and 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to SDK client integration.	21/07/2016	7.8	CVE-2016-3532
oracle - crm_technical_foundation	Unspecified vulnerability in the Oracle CRM Technical Foundation component in Oracle E-Business Suite 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to Remote Launch.	21/07/2016	7.8	CVE-2016-3535
oracle - marketing	Unspecified vulnerability in the Oracle Marketing component in Oracle E-Business Suite 12.1.1, 12.1.2, and 12.1.3 allows remote attackers to affect confidentiality and integrity via vectors related to Deliverables.	21/07/2016	7.8	CVE-2016-3536
oracle - agile_product_lifecycle_management_fra_integrator	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote authenticated users to affect integrity and availability via vectors related to File Folders / Attachment, a different vulnerability than CVE-2016-3538.	21/07/2016	7.5	CVE-2016-3538
oracle - agile_product_lifecycle_management_fra_integrator	Unspecified vulnerability in the Oracle Agile PLM component in Oracle Supply Chain Products Suite 9.3.4 and 9.3.5 allows remote authenticated users to affect integrity and availability via vectors related to File Folders / Attachment, a different vulnerability than CVE-2016-3538.	21/07/2016	7.5	CVE-2016-3539
oracle - integrated_lights_out_manager_firmware	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors.	21/07/2016	7.5	CVE-2016-5445
oracle - integrated_lights_out_manager_firmware	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to Infrastructure.	21/07/2016	7.5	CVE-2016-5446
oracle - integrated_lights_out_manager_firmware	Unspecified vulnerability in the ILOM component in Oracle Sun Systems Products Suite 3.0, 3.1, and 3.2 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to IPMI.	21/07/2016	7.5	CVE-2016-5453
oracle - peoplesoft_enterprise_peopletools	Unspecified vulnerability in the PeopleSoft Enterprise PeopleTools component in Oracle PeopleSoft Products 8.54 and 8.55 allows local users to affect confidentiality, integrity, and availability via vectors related to install and Packaging.	21/07/2016	7.5	CVE-2016-5472
harfbuzz_project - harfbuzz	Hi- or layout-guess-table hit in Harfbuzz before 1.0.5 allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via crafted data, a different vulnerability than CVE-2016-2092.	19/07/2016	7.5	CVE-2016-8947
missys - fusioncapital_opics_plus	Missys FusionCapital Opics Plus allows remote authenticated users to gain privileges via a man-in-the-middle attack that modifies the <code>writeReleaseOut</code> parameter.	19/07/2016	8.5	CVE-2016-5654
objective_systems - asntc	Integer overflow in the <code>rmMemHeapAlloc</code> function in <code>asntnrt.lib</code> in Objective Systems ASNTIC for C/C++ before 7.0.2 allows content-dependent attackers to execute arbitrary code or cause a denial of service (heap-based buffer overflow), on a system running an application compiled by ASNTIC via crafted ASNTIC data.	19/07/2016	10.0	CVE-2016-5080
ibm - traveler	IBM Traveler 8.x and 8.x before 9.0.1.12 allows remote authenticated users to read arbitrary files or cause a denial of service (memory consumption) via XML data containing an external entity declaration in conjunction with an entity reference, related to <code>xml:External-Entity (XSL) issue</code> .	17/07/2016	8.5	CVE-2016-3939
csso - ios_w	Cisco IOS XR 5.x through 5.2.5 on NCS 6000 devices allows remote attackers to cause a denial of service (buffer consumption and Route Processor reload) via crafted SSH traffic, aka Bug-ID CSCu076919.	16/07/2016	7.8	CVE-2016-1426
csso - ios_w	The CLI in Cisco IOS XR 6.x through 6.5 allows local users to execute arbitrary OS commands in a privileged context by leveraging unspecified console access, aka Bug-ID CSCu079721.	15/07/2016	7.5	CVE-2016-1456
hp - hp	HP iMC PLAT before 7.2 (E0403P04), iMC EAD before 7.2 (E0405P05), iMC APM before 7.2 (E0401P04), iMC NTA before 7.2 (E0401P01), iMC BMC before 7.2 (E0402P02), and iMC UAM before 7.2 (E0405P05) allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.	15/07/2016	7.5	CVE-2016-4177
schneider-electric - pdco_digital_sentry_video_management_system_firmware	Schneider Electric Pdco Digital Sentry Video Management System with firmware before 7.14 has hardcoded credentials, which allows remote attackers to obtain access, and consequently execute arbitrary code, via unspecified vectors.	15/07/2016	10.0	CVE-2016-4520
schneider-electric - sohmachine_hvac_firmware	An unspecified ActiveX control in Schneider Electric SoMachine HVAC Programming Software for M171/M172 Controllers before 2.1.0 allows remote attackers to execute arbitrary code via unknown vectors, related to the <code>INTERFACEDATA_FOR_UNREGISTERED_CALLER</code> (aka safe for script) file.	15/07/2016	7.5	CVE-2016-4529

Historico de vulnerabilidades de Julio del 2016

Primary Vendor / Product	Description	Published	CVE Score	Source & Patch Info
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 and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3252, CVE-2016-3254, and CVE-2016-3260.	12/07/2016	7.2	CVE-2016-3249
microsoft -- windows_10	The kernel-mode drivers in Microsoft Windows Server 2012 and Windows 10 Gold and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."	12/07/2016	7.2	CVE-2016-3250
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 and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3249, CVE-2016-3254, and CVE-2016-3260.	12/07/2016	7.2	CVE-2016-3253
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 and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3249, CVE-2016-3252, and CVE-2016-3260.	12/07/2016	7.2	CVE-2016-3254
microsoft -- edge	The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Internet Explorer 9 through 11, Microsoft Edge, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3248.	12/07/2016	9.3	CVE-2016-3249
microsoft -- edge	The Microsoft (1) JScript 9, (2) VBScript, and (3) Chakra JavaScript engines, as used in Microsoft Internet Explorer 9, Microsoft Edge, and other products, allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability."	12/07/2016	9.3	CVE-2016-3250
microsoft -- edge	Microsoft Internet Explorer 9 through 11 and Microsoft Edge allow remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Microsoft Browser Memory Corruption Vulnerability."	12/07/2016	7.6	CVE-2016-3264
microsoft -- edge	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3260.	12/07/2016	9.3	CVE-2016-3265
microsoft -- edge	The Chakra JavaScript engine in Microsoft Edge allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted web site, aka "Scripting Engine Memory Corruption Vulnerability," a different vulnerability than CVE-2016-3265.	12/07/2016	9.3	CVE-2016-3269
microsoft -- outlook	Microsoft Outlook 2010 SP2, 2013 SP1, 2013 RT SP1, and 2016 allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/07/2016	9.3	CVE-2016-3178
microsoft -- office	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, and Word Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/07/2016	9.3	CVE-2016-3180
microsoft -- office	Microsoft Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Word for Mac 2011, Word 2016 for Mac, Word Automation Services on SharePoint Server 2010 SP2, and Office Web Apps 2010 SP2 allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/07/2016	9.3	CVE-2016-3181
microsoft -- office	Microsoft Word 2007 SP3, Office 2010 SP2, Word 2010 SP2, Word 2013 SP1, Word 2013 RT SP1, Word 2016, Word for Mac 2011, Word 2016 for Mac, Office Compatibility Pack SP3, Word Viewer, Word Automation Services on SharePoint Server 2010 SP2, Word Automation Services on SharePoint Server 2013 SP1, SharePoint Server 2013, Office Web Apps 2010 SP2, Office Web Apps 2013 SP1, and Office Online Server allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/07/2016	9.3	CVE-2016-3182
microsoft -- word_viewer	Microsoft Word Viewer allows remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/07/2016	9.3	CVE-2016-3228
microsoft -- excel	Microsoft Excel 2007 SP3, Excel 2010 SP2, Excel 2013 SP1, Excel 2013 RT SP1, Excel 2016, Excel for Mac 2011, Excel 2016 for Mac, Office Compatibility Pack SP3, and Excel Viewer allow remote attackers to execute arbitrary code via a crafted Office document, aka "Microsoft Office Memory Corruption Vulnerability."	12/07/2016	9.3	CVE-2016-3184
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 and 1511 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3249, CVE-2016-3252, and CVE-2016-3254.	12/07/2016	7.2	CVE-2016-3248
inercorp -- line	Unrestricted search path vulnerability in LINE and LINE Installer 4.7.2 and earlier on Windows allows local users to gain privileges via a Trojan horse DLL in an unsecured directory.	11/07/2016	7.2	CVE-2016-4831
symantec -- client_intrusion_detection_system	The Client Intrusion Detection System (CIDS) driver before 15.0.6 in Symantec Endpoint Protection (SEP) and before 15.1.2 in Norton Security allows remote attackers to cause a denial of service (memory corruption and system crash) via a malformed nullable executable (PE) file.	11/07/2016	7.1	CVE-2016-5308
google -- android	Unspecified vulnerability in the Qualcomm components in Android before 2016-07-05 allows attackers to gain privileges via a crafted application.	10/07/2016	10.0	CVE-2016-7452
google -- android	The vid_dec_set_meta_buffers function in drivers/video/msm/vid/common/dec/vidc.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate the number of buffers, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28598501 and Qualcomm internal bug CR563654.	10/07/2016	9.3	CVE-2016-9777
google -- android	The vid_dec_set_h264_mv_buffers function in drivers/video/msm/vid/common/dec/vidc.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate the number of buffers, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28598515 and Qualcomm internal bug CR564694.	10/07/2016	9.3	CVE-2016-9778
google -- android	arch/arm/mach-msm/gpdrv/mem_audb_jon.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices allows attackers to obtain sensitive information from kernel memory via a crafted offset, aka Android internal bug 28598347 and Qualcomm internal bug CR548676.	10/07/2016	9.3	CVE-2016-9779
google -- android	drivers/video/msm/vid/ndvs3_crt.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5, 5X, and 6P devices does not validate start and length values, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28620014 and Qualcomm internal bug CR542722.	10/07/2016	9.3	CVE-2016-9780
google -- android	Buffer overflow in drivers/video/bozap.c in the Qualcomm components in Android before 2016-07-05 on Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28410313 and Qualcomm internal bug CR556471.	10/07/2016	9.3	CVE-2016-9781
google -- android	drivers/media/platform/msm/camera_v2/sensor/actuator/msm_actuator.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate direction and step parameters, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28613131 and Qualcomm internal bug CR513495.	10/07/2016	9.3	CVE-2016-9782
google -- android	drivers/media/platform/msm/camera_v2/sensor/csi/msm_ccic.c in the Qualcomm components in Android before 2016-07-05 on Nexus 7 (2013) devices does not validate certain values, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28441913 and Qualcomm internal bug CR511189.	10/07/2016	9.3	CVE-2016-9783
google -- android	Multiple buffer overflows in drivers/media/flash/ahbq.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allow attackers to gain privileges via a crafted application, aka Android internal bug 28442449 and Qualcomm internal bug CR581347.	10/07/2016	9.3	CVE-2016-9784
google -- android	drivers/mmi/apeccs.c in the Qualcomm components in Android before 2016-07-05 on Nexus 7 (2013) devices does not validate addresses before copying data, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28449032 and Qualcomm internal bug CR545747.	10/07/2016	9.3	CVE-2016-9785
google -- android	Heap-based buffer overflow in drivers/media/platform/msm/camera_v2/sensor/actuator/msm_actuator.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28552760 and Qualcomm internal bug CR545079.	10/07/2016	9.3	CVE-2016-9786
google -- android	Integer overflow in drivers/mmi2/gpuccs.c in the Qualcomm components in Android before 2016-07-05 on Nexus 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28514565 and Qualcomm internal bug CR545764.	10/07/2016	9.3	CVE-2016-9787
google -- android	Multiple buffer overflows in the voice drivers in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices allow attackers to gain privileges via a crafted application, aka Android internal bug 28571112 and Qualcomm internal bug CR548872.	10/07/2016	9.3	CVE-2016-9788
google -- android	The (1) alic and (2) free APIs in arch/arm/mach-msm/gpdrv/mem_audb_jon.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices do not validate parameters, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28749392 and Qualcomm internal bug CR554425.	10/07/2016	9.3	CVE-2016-9789
google -- android	drivers/mmi/core/dbgdbg.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate pointers used in read and write operations, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28769136 and Qualcomm internal bug CR545716.	10/07/2016	9.3	CVE-2016-9790
google -- android	arch/arm/mach-msm/lpc_router.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices uses an incorrect integer data type, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28769399 and Qualcomm internal bug CR550006.	10/07/2016	9.3	CVE-2016-9792
google -- android	platform/msm_shared/mmc in the Qualcomm components in Android before 2016-07-05 on Nexus 7 (2013) devices mishandles the power-on write protect feature, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28821253 and Qualcomm internal bug CR580567.	10/07/2016	9.3	CVE-2016-9793
google -- android	app/aboot/aboot.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices does not properly check for an integer overflow, which allows attackers to bypass intended access restrictions via crafted start and size values, aka Android internal bug 28820720 and Qualcomm internal bug CR568357, a related issue to CVE-2016-4235.	10/07/2016	10.0	CVE-2016-9795
google -- android	app/aboot/aboot.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate the page size in the kernel header, which allows attackers to bypass intended access restrictions via a crafted boot image, aka Android internal bug 28820722 and Qualcomm internal bug CR684756.	10/07/2016	9.3	CVE-2016-9796
google -- android	platform/msm_shared/dev_tree in the Qualcomm bootloader in Android before 2016-07-05 on Nexus 5 devices does not check the relationship between tag addresses and aboot addresses, which allows attackers to cause a denial of service (DS out-of-range) via a crafted application, aka Android internal bug 28821248 and Qualcomm internal bug CR681965.	10/07/2016	7.1	CVE-2016-9798
google -- android	The makefile in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices omits the -fno-stack-overflow option to gcc, which might allow attackers to gain privileges via a crafted application that leverages incorrect compiler optimization of an integer-overflow protection mechanism, aka Android internal bug 28821731 and Qualcomm internal bug CR690336.	10/07/2016	9.3	CVE-2016-9799
google -- android	Integer overflow in lib/heap/heap.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28821250 and Qualcomm internal bug CR705078.	10/07/2016	9.3	CVE-2016-9800
google -- android	Multiple integer overflows in lib/hibltd/hibltd_pwc.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices allow attackers to gain privileges via a crafted application, aka Android internal bug 28822060 and Qualcomm internal bug CR705078.	10/07/2016	9.3	CVE-2016-9801
google -- android	Multiple integer overflows in lib/hibltd/hibltd.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allow attackers to gain privileges via a crafted application, aka Android internal bug 28821965 and Qualcomm internal bug CR705078.	10/07/2016	9.3	CVE-2016-9802
google -- android	arch/arm4/include/asm/fgtable.h in the Linux kernel before 3.15-rc5-next-20140519, as used in Android before 2016-07-05 on Nexus 5X and 6P devices, mishandles execute-only pages, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28512920.	10/07/2016	9.3	CVE-2016-9803
google -- android	Integer overflow in app/aboot/aboot.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices allows attackers to bypass intended access restrictions via a crafted block count and block size of a sparse header, aka Android internal bug 28821865 and Qualcomm internal bug CR811913.	10/07/2016	9.3	CVE-2016-9808
google -- android	The aboot implementation in the Qualcomm components in Android before 2016-07-05 on Nexus 6P devices omits the recovery PIN feature, which has unspecified impact and attack vectors, aka Android internal bug 28822677 and Qualcomm internal bug CR980867.	10/07/2016	9.3	CVE-2016-9809
google -- android	platform/msm_shared/partition_parser.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices does not validate certain GUID Partition Table (GPT) data, which allows attackers to bypass intended access restrictions via a crafted MultiMediaCard (MMC), aka Android internal bug 28822878 and Qualcomm internal bug CR823461.	10/07/2016	9.3	CVE-2016-9801
google -- android	Multiple integer overflows in app/aboot/aboot.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 and 7 (2013) devices allow attackers to bypass intended access restrictions via a crafted image, aka Android internal bug 28842418 and Qualcomm internal bug CR811930.	10/07/2016	9.3	CVE-2016-9802
google -- android	platform/msm_shared/boot_verifier.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers to bypass intended access restrictions via a digest with trailing data, aka Android internal bug 28822807 and Qualcomm internal bug CR902966.	10/07/2016	9.3	CVE-2016-9802
google -- android	drivers/gpu/msm/agg.c in the MSM graphics driver (aka GPU driver) for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, mishandles the KGSL_MEMFLAGS_OPUREDONLY flag, which allows attackers to gain privileges by leveraging accidental read write mappings, aka Qualcomm internal bug CR988991.	10/07/2016	9.3	CVE-2016-2067

Histórico de vulnerabilidades de Julio del 2016

Primary Vendor / Product	Description	Published	CVSS Score	Source & Patch Info
google - android	The MSM QDSP audio driver (aka sound 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 (Integer overflow, and buffer overflow or buffer over-read) via a crafted application that performs a (1) AUDIO_EFFECTS_WRITE or (2) AUDIO_EFFECTS_READ operation. aka Qualcomm internal bug CR100609	10/07/2016	9.3	CVE-2016-2098
google - android	The Qualcomm camera driver in Android before 2016-07-05 on Nexus 5X, 6, 6P, and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 2780772 and Qualcomm internal bug CR1001092.	10/07/2016	9.3	CVE-2016-2101
google - android	drivers/usb/gadget/_serial.c in the Qualcomm USB driver in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a large size in a GSER_IOCTL ioctl call, aka Android internal bug 27657963 and Qualcomm internal bug CR100944.	10/07/2016	9.3	CVE-2016-2107
google - android	The Qualcomm GPU driver in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application. aka Android internal bug 28084793 and Qualcomm internal bug CR1009067.	10/07/2016	9.4	CVE-2016-2109
google - android	hwcomposer/HTPparse.cpp in liblogtagright in mediaserver in Android 6.x before 2016-07-01 does not validate a certain section length, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file. aka internal bug 28133306.	10/07/2016	9.3	CVE-2016-2105
google - android	libextractor.cpp in liblogtagright in mediaserver in Android 6.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 does not validate a certain offset value, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file. aka internal bug 28175045.	10/07/2016	10.0	CVE-2016-2106
google - android	Integer overflow in codes/ortp2/rtplib/source/rtplibout_storage.c in liblogtagright in mediaserver in Android 4.x before 4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file. aka internal bug 28132266.	10/07/2016	9.3	CVE-2016-2107
google - android	media/libmediaplayerservice/huplayer/GenetSource.cpp in mediaserver 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 2016-07-01 does not validate certain track data, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file. aka internal bug 28791941.	10/07/2016	9.3	CVE-2016-2108
google - android	The H.264 decoder in mediaserver in Android 6.x before 2016-07-01 does not initialize certain slice data, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28167061.	10/07/2016	7.5	CVE-2016-1741
google - android	hwcomposer/02644_process_intra_mbc in mediaserver in Android 6.x before 2016-07-01 mishandles intra mode, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28165659.	10/07/2016	7.5	CVE-2016-1742
google - android	hwcomposer/02644_app.c in mediaserver in Android 6.x before 2016-07-01 does not initialize certain data structures, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 27907656.	10/07/2016	7.5	CVE-2016-1743
google - android	Multiple buffer overflows in mediaserver 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 2016-07-01 allow attackers to gain privileges via a crafted application that provides an AudioEffect reply, as demonstrated by obtaining Signature or SignatureOfSystem access. aka internal bug 28174666.	10/07/2016	7.5	CVE-2016-1745
google - android	Use-after-free vulnerability in the mpeg-video-vc1c video component in mediaserver 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 2016-07-01 allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOfSystem access. aka internal bug 27897807.	10/07/2016	7.5	CVE-2016-1746
google - android	Use-after-free vulnerability in the mpeg-video-vc1c video component in mediaserver 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 2016-07-01 allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOfSystem access. aka internal bug 27901498.	10/07/2016	10.0	CVE-2016-1747
google - android	The sockets subsystem in Android 6.x before 2016-07-01 allows attackers to bypass intended system-call restrictions via a crafted application that makes a ioctl call. aka internal bug 28121804.	10/07/2016	7.5	CVE-2016-1748
google - android	libBinder/Parcel.cpp in the Parcel 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 2016-07-01 does not validate the return value of the dup system call, which allows attackers to bypass an isolation exception mechanism via a crafted application. aka internal bug 28099562.	10/07/2016	7.5	CVE-2016-1750
google - android	internal/app/ChooserActivity.java in the ChooserTarget service in Android 6.x before 2016-07-01 mishandles target security checks, which allows attackers to gain privileges via a crafted application. aka internal bug 28384423.	10/07/2016	7.5	CVE-2016-1752
google - android	Mediaserver in Android 6.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 does not limit process memory usage, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 28015488.	10/07/2016	7.8	CVE-2016-1754
google - android	hwcomposer/02644_panic_poller.c in mediaserver in Android 6.x before 2016-07-01 does not properly select concealment frames, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 28270138.	10/07/2016	7.8	CVE-2016-1755
google - android	hwcomposer/02612.c in mediaserver 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 2016-07-01 does not validate the number of partitions, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted media file, aka internal bug 28056125.	10/07/2016	7.8	CVE-2016-1756
google - android	Multiple buffer overflows in liblogtagright in DecLoader 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 2016-07-01 allow attackers to gain privileges via a crafted application that provides a long filename, aka internal bug 27880771.	10/07/2016	9.3	CVE-2016-1758
google - android	The sockets subsystem in Android 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows attackers to gain privileges via a crafted application that uses (1) the AF_MGM_SOCKET class or (2) another socket class that is unrecognized by libLinux. aka internal bug 28812700.	10/07/2016	9.3	CVE-2016-1762
google - android	libextractor.cpp in liblogtagright in mediaserver 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 2016-07-01 does not check whether memory allocation succeeds, which allows remote attackers to cause a denial of service (device hang or reboot) via a crafted file, aka internal bug 28471206.	10/07/2016	7.8	CVE-2016-1756
google - android	The MediaTek Wi-Fi driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application. aka Android internal bug 28169383 and MediaTek internal bug ALP50268926.	10/07/2016	9.3	CVE-2016-1767
google - android	The Qualcomm performance component in Android before 2016-07-05 on Nexus 5, 5X, 6P, and 7 (2013) devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28172137 and Qualcomm internal bug CR1010644.	10/07/2016	9.3	CVE-2016-1768
google - android	The NVIDIA video driver in Android before 2016-07-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application. aka Android internal bug 28174056.	10/07/2016	9.3	CVE-2016-1769
google - android	The MediaTek drivers in Android before 2016-07-05 on Android One devices allow attackers to gain privileges via a crafted application. aka Android internal bug 28346753 and MediaTek internal bug ALP502703102.	10/07/2016	9.3	CVE-2016-1770
google - android	The MediaTek drivers in Android before 2016-07-05 on Android One devices allow attackers to gain privileges via a crafted application. aka Android internal bug 28008188 and MediaTek internal bug ALP502703102.	10/07/2016	9.3	CVE-2016-1771
google - android	The MediaTek drivers in Android before 2016-07-05 on Android One devices allow attackers to gain privileges via a crafted application. aka Android internal bug 28008188 and MediaTek internal bug ALP502703102.	10/07/2016	9.3	CVE-2016-1772
google - android	The MediaTek drivers in Android before 2016-07-05 on Android One devices allow attackers to gain privileges via a crafted application. aka Android internal bug 28008188 and MediaTek internal bug ALP502703102.	10/07/2016	9.3	CVE-2016-1773
google - android	The MediaTek drivers in Android before 2016-07-05 on Android One devices allow attackers to gain privileges via a crafted application. aka Android internal bug 28008188 and MediaTek internal bug ALP502703102.	10/07/2016	9.3	CVE-2016-1774
google - android	The kernel filesystem implementation in Android before 2016-07-05 on Nexus 5X, Nexus 6P, Nexus Player, and Pixel C devices allows attackers to gain privileges via a crafted application. aka internal bug 28088279.	10/07/2016	9.4	CVE-2016-1775
google - android	CONJUNCTION.invariant_held_notimpl.c in the Qualcomm Wi-Fi driver in Android before 2016-07-01 on Nexus 7 (2013) devices mishandles userspace data copying, which allows attackers to gain privileges via a crafted application, aka Android internal bug 27725704 and Qualcomm internal bug CR61027.	10/07/2016	9.3	CVE-2016-1792
google - android	The NVIDIA camera driver in Android before 2016-07-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application. aka Android internal bug 28026025.	10/07/2016	9.3	CVE-2016-1793
google - android	The MediaTek power driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application. aka Android internal bug 28084722 and MediaTek internal bug ALP502677244.	10/07/2016	9.3	CVE-2016-1795
google - android	The MediaTek power driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application. aka Android internal bug 28084843 and MediaTek internal bug ALP502677244.	10/07/2016	9.3	CVE-2016-1796
google - android	The Qualcomm Wi-Fi driver in Android before 2016-07-05 on Nexus 5X devices allows attackers to gain privileges via a crafted application. aka Android internal bug 28089580 and Qualcomm internal bug CR1004450.	10/07/2016	9.3	CVE-2016-1797
google - android	The MediaTek hardware sensor driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application. aka Android internal bug 28134490 and MediaTek internal bug ALP502703105.	10/07/2016	9.3	CVE-2016-1798
google - android	The MediaTek video driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application. aka Android internal bug 28137017 and MediaTek internal bug ALP50269739.	10/07/2016	9.3	CVE-2016-1799
google - android	The MediaTek video driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application. aka Android internal bug 28137017 and MediaTek internal bug ALP50269739.	10/07/2016	9.3	CVE-2016-1800
google - android	The MediaTek GPS driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application. aka Android internal bug 28137014 and MediaTek internal bug ALP50268803.	10/07/2016	9.3	CVE-2016-1801
google - android	The kernel filesystem implementation in Android before 2016-07-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application. aka internal bug 28271368.	10/07/2016	9.3	CVE-2016-1802
google - android	The kernel filesystem implementation in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application. aka internal bug 2858834.	10/07/2016	9.3	CVE-2016-1803
google - android	The MediaTek power management driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28332766 and MediaTek internal bug ALP502694410.	10/07/2016	9.3	CVE-2016-1804
google - android	The MediaTek power management driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application, aka Android internal bug 28333002 and MediaTek internal bug ALP502694412.	10/07/2016	9.3	CVE-2016-1805
google - android	The MediaTek display driver in Android before 2016-07-05 on Android One devices allows attackers to gain privileges via a crafted application. aka Android internal bug 28402341 and MediaTek internal bug ALP502715341.	10/07/2016	9.3	CVE-2016-1806
google - android	The serial peripheral interface driver in Android before 2016-07-05 on Nexus 5X and 6P devices allows attackers to gain privileges via a crafted application. aka internal bug 28402106.	10/07/2016	9.3	CVE-2016-1807
google - android	The serial peripheral interface driver in Android before 2016-07-05 on Pixel C devices allows attackers to gain privileges via a crafted application. aka internal bug 28400079.	10/07/2016	9.3	CVE-2016-1808
google - android	The kernel video driver in Android before 2016-07-05 on Nexus 9 devices allows attackers to gain privileges via a crafted application. aka internal bug 28447556.	10/07/2016	9.3	CVE-2016-1811
google - android	libc in Android 4.x before 4.4.4 allows remote attackers to cause a denial of service (device hang or reboot) via a crafted file, aka internal bug 28340702.	10/07/2016	7.3	CVE-2016-1818
libpng - libpng	Unspecified vulnerability in libpng before 1.6.20, as used 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 2016-07-01, allows attackers to gain privileges via a crafted application, as demonstrated by obtaining Signature or SignatureOfSystem access. aka internal bug 28206069.	10/07/2016	7.5	CVE-2016-1751

Histórico de vulnerabilidades de Julio del 2016

Semana 04/07/2016				
Primary Vendor - Product	Description	Published	CVSS Score	Source & Patch Info
apache - commons_fileupload	The MultiPartStream class in Apache Commons Fileupload before 3.2.2, as used in Apache Tomcat 7.x before 7.0.70, 8.x before 8.0.36, 8.5.x before 8.5.3, and 9.x before 9.0.0.M7 and other products, allows remote attackers to cause a denial of service (CPU consumption) via a long boundary string.	04/07/2016	7.8	CVE-2016-3092
apache - struts	The REST plugin in Apache Struts 2.3.20 through 2.3.28.1 allows remote attackers to execute arbitrary code via a crafted exception.	04/07/2016	7.5	CVE-2016-4438
apple - airport_base_station_firmware	Apple Airport Base Station Firmware before 7.6.7 and 7.7.x before 7.7.7 misparses DNS data, which allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors.	02/07/2016	10.0	CVE-2015-7029
cisco - evolved_programmable_network_manager	The API in Cisco Prime Infrastructure 1.2 through 3.0 and Evolved Programmable Network Manager (EPNM) 1.2 allows remote attackers to execute arbitrary code or obtain sensitive management information via a crafted HTTP request, as demonstrated by discovering managed device credentials, aka Bug ID CSCvu10231.	02/07/2016	10.0	CVE-2016-1480
cisco - epc3928_firmware	goform/WClientMAMList on Cisco EPC3928 devices allows remote attackers to cause a denial of service (device crash) via a long %s_sortWireless parameter, related to a "Gateway Client List Denial of Service" issue, aka Bug ID CSCuc93868.	03/07/2016	7.8	CVE-2016-1328
cisco - epc3928_firmware	goform/DocIntr_system on Cisco EPC3928 devices allows remote attackers to cause a denial of service (device crash) via a long languageSelect parameter, related to a "Gateway HTTP Corruption Denial of Service" issue, aka Bug ID CSCuc93868.	03/07/2016	7.8	CVE-2016-1336
cisco - firelight_system_software	Cisco Firepower System Software 6.0.0 through 6.1.0 has a hardcoded account, which allows remote attackers to obtain CLI access by leveraging knowledge of the password, aka Bug ID CSCur64238.	02/07/2016	7.5	CVE-2016-1376
cisco - prime_collaboration_provisioning	Cisco Prime Collaboration Provisioning 10.6 SP2 (aka 10.6.0.10602) mishandles LDAP authentication, which allows remote attackers to obtain administrator privileges via a crafted login attempt, aka Bug ID CSCuc97513.	02/07/2016	10.0	CVE-2016-1416
cisco - prime_infrastructure	The administrative web interface in Cisco Prime Infrastructure (PI) before 3.1.1 allows remote authenticated users to execute arbitrary commands via crafted field values, aka Bug ID CSCuc92269.	07/07/2016	9.0	CVE-2016-1444
citron - elcsoft	Stack-based buffer overflow in ELCSimulator in Laton ELCSoft 2.4.01 and earlier allows remote attackers to execute arbitrary code via a long packet.	03/07/2016	7.5	CVE-2016-4513
ibm - power_hardware_management_console	IBM Power Hardware Management Console (HMC) 7.3 through 7.3.0 SP7, 7.9 through 7.9.0 SP3, 8.1 through 8.1.0 SP3, 8.2 through 8.2.0 SP2, 8.3 through 8.3.0 SP2, 8.4 through 8.4.0 SP1, and 8.5.0 allows physically proximate attackers to obtain root access via unspecified vectors.	07/07/2016	7.2	CVE-2016-6220
ibm - urbnocode_deploy	The agents in IBM UrbanCode Deploy 6.x before 6.0.1.14, 6.1.x before 6.1.3.3, and 6.2.x before 6.2.1.1 do not verify a server's identity in a JMS session or an HTTP session, which allows local users to obtain root access to arbitrary agents via unspecified vectors.	07/07/2016	7.2	CVE-2016-6271
ibm - watson_developer_cloud	The IBM Watson Developer Cloud services on Bluemix platforms do not properly generate random numbers for service-instance credentials, which makes it easier for remote attackers to defeat cryptographic protection mechanisms via a brute-force attack.	02/07/2016	7.5	CVE-2016-6391
linux - linux_kernel	The usbip_recv_xbuff function in drivers/usb/usbip/usbip_common.c in the Linux kernel before 4.5.3 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via a crafted length value in a USB/IP packet.	03/07/2016	10.0	CVE-2016-3905
linux - linux_kernel	The compat_IP_TOS_REPLACE setssockopt implementation in the netfilter subsystem in the Linux kernel before 4.6.3 allows local users to gain privileges or cause a denial of service (memory corruption) by leveraging in-container root access to provide a crafted effort value that triggers an unintended decrement.	03/07/2016	7.2	CVE-2016-4997
meinberg - ims-lantime_m1000	Stack-based buffer overflow in the NTP time-server interface on Meinberg IMS-LANTIME M3000, IMS-LANTIME M1000, IMS-LANTIME M500, LANTIME M900, LANTIME M600, LANTIME M400, LANTIME M300, LANTIME M200, LANTIME M100, SyncFire 1100, and LCES devices with firmware before 6.20.004 allows remote attackers to obtain sensitive information, modify data, or cause a denial of service via a crafted parameter in a POST request.	03/07/2016	7.5	CVE-2016-3962
meinberg - ims-lantime_m3000	Multiple stack-based buffer overflows in the NTP time-server interface on Meinberg IMS-LANTIME M3000, IMS-LANTIME M1000, IMS-LANTIME M500, LANTIME M900, LANTIME M600, LANTIME M400, LANTIME M300, LANTIME M200, LANTIME M100, SyncFire 1100, and LCES devices with firmware before 6.20.004 allow remote attackers to obtain sensitive information, modify data, or cause a denial of service via a crafted parameter in a POST request.	03/07/2016	7.5	CVE-2016-3988
meinberg - ims-lantime_m1000	The NTP time-server interface on Meinberg IMS-LANTIME M3000, IMS-LANTIME M1000, IMS-LANTIME M500, LANTIME M900, LANTIME M600, LANTIME M400, LANTIME M300, LANTIME M200, LANTIME M100, SyncFire 1100, and LCES devices with firmware before 6.20.004 allows remote authenticated users to obtain root privileges for writing to unspecified scripts, and consequently obtain sensitive information or modify data, by leveraging access to the nobody account.	03/07/2016	8.5	CVE-2016-3989
microfocus - rumba	Multiple stack-based buffer overflows in COM objects in Micro Focus Rumba 9.4.x before 9.4 HF 13960 allow remote attackers to execute arbitrary code via (1) the NetworkName property value to ObjectXSNAConfig.ObjectXSNAConfig in iconfig.dll, (2) the CPName property value to ObjectXSNAConfig.ObjectXSNAConfig in iconfig.dll, (3) the PrinterName property value to ProfileEditor.ProfileControl in Profile.dll, (4) the data argument to the WriteRecords function in FTFSrvLib.AS400FvxBFF in FvxBFF.dll, (5) the Serialized property value to NMSECCOMPARAMSLib.SS3 in NMSECCOMPParams.dll, (6) the UserName property value to NMSECCOMPARAMSLib.FirewallProxy in NMSECCOMPParams.dll, (7) the LUName property value to ProfileEditor.APSNACControl in Profile.dll, (8) the newVal argument to the Load function in FTFSrvLib.SrvgSession in FTFSrvLib.dll, or (9) a long Host field in the FTP Client.	02/07/2016	10.0	CVE-2016-1600
microfocus - rumba	Stack-based buffer overflow in the PlayMacro function in ObjectXMacro.ObjectXMacro in WinMacCtl.exe in Micro Focus Rumba 9.x before 9.3 HF 11997 and 9.4.x before 9.4 HF 12815 allows remote attackers to execute arbitrary code via a long MacroName argument. NOTE: some references mention CVE-2016-5226 but that is not a correct ID for any Rumba vulnerability.	02/07/2016	10.0	CVE-2016-5228
openvswitch - openvswitch	Buffer overflow in lib/flow.c in openvswitch in Open vSwitch 2.2.x and 2.3.x before 2.3.3 and 2.4.x before 2.4.1 allows remote attackers to execute arbitrary code via crafted MPLS packets, as demonstrated by a long string in an openvswitch command.	03/07/2016	7.5	CVE-2016-2074
phpmyadmin - phpmyadmin	SQL injection vulnerability in libraries/central_columns.lib.php in phpMyAdmin 4.x before 4.4.15.7 and 4.6.x before 4.6.3 allows remote attackers to execute arbitrary SQL commands via a crafted database name that is mishandled in a central column query.	02/07/2016	7.5	CVE-2016-5707
phpmyadmin - phpmyadmin	phpMyAdmin 4.0.x before 4.0.10.16, 4.4.x before 4.4.15.7, and 4.6.x before 4.6.3 does not properly choose delimiters to prevent use of the preg_replace (aka eval) modifier, which might allow remote attackers to execute arbitrary PHP code via a crafted string, as demonstrated by the table search and replace implementation.	02/07/2016	7.5	CVE-2016-5734