Histórico de vulnerabilidades de Agosto do 2016

Semana 29/08/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
python -- python	Integer overflow in the get_data function in zipimport.c in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 allows remote attackers to have unspecified impact via a negative data size value, which triggers a heap-based buffer overflow.	02/09/2016	10.0	CVE-2016-5636
cisco -- small_business_220_series_smart_plus_switches	Cisco Small Business 220 devices with firmware before 1.0.1.1 have a hardcoded SNMP community, which allows remote attackers to read or modify SNMP objects by leveraging knowledge of this community, aka Bug ID CSCuz76216.	01/09/2016	10.0	CVE-2016-1473
netgear -- readynas_surveillance	__debugging_center_utils___.php in NUUO NVRmini 2 1.7.5 through 3.0.0, NUUO NVRsolo 1.7.5 through 3.0.0, and NETGEAR ReadyNAS Surveillance 1.1.1 through 1.4.1 allows remote attackers to execute arbitrary PHP code via the log parameter.	31/08/2016	10.0	CVE-2016-5674
netgear -- readynas_surveillance	handle_daylightsaving.php in NUUO NVRmini 2 1.7.5 through 3.0.0, NUUO NVRsolo 1.0.0 through 3.0.0, NUUO Crystal 2.2.1 through 3.2.0, and NETGEAR ReadyNAS Surveillance 1.1.1 through 1.4.1 allows remote attackers to execute arbitrary PHP code via the NTPServer parameter.	31/08/2016	10.0	CVE-2016-5675
netgear -- readynas_surveillance	cgi-bin/cgi_main in NUUO NVRmini 2 1.7.6 through 3.0.0 and NETGEAR ReadyNAS Surveillance 1.1.2 allows remote authenticated users to execute arbitrary commands via shell metacharacters in the sn parameter to the transfer_license command.	31/08/2016	9.0	CVE-2016-5679
netgear -- readynas_surveillance	Stack-based buffer overflow in cgi-bin/cgi_main in NUUO NVRmini 2 1.7.6 through 3.0.0 and NETGEAR ReadyNAS Surveillance 1.1.2 allows remote authenticated users to execute arbitrary code via the sn parameter to the transfer_license command.	31/08/2016	9.0	CVE-2016-5680
nuuo -- nvrmini_2	NUUO NVRmini 2 1.0.0 through 3.0.0 and NUUO NVRsolo 1.0.0 through 3.0.0 have hardcoded root credentials, which allows remote attackers to obtain administrative access via unspecified vectors.	31/08/2016	10.0	CVE-2016-5678
linux -- linux_kernel	Heap-based buffer overflow in the wcnss_wlan_write function in drivers/net/wireless/wcnss/wcnss_wlan.c in the wcnss_wlan device 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 by writing to /dev/wcnss_wlan with an unexpected amount of data.	30/08/2016	10.0	CVE-2016-5342
linux -- linux_kernel	Multiple integer overflows in the MDSS driver for the Linux kernel 3.x, as used in Qualcomm Innovation Center (QuIC) Android contributions for MSM devices and other products, allow attackers to cause a denial of service or possibly have unspecified other impact via a large size value, related to mdss_compat_utils.c, mdss_fb.c, and mdss_rotator.c.	30/08/2016	10.0	CVE-2016-5344
mac-telnet_project -- mac-telnet	Buffer overflow in the handle_packet function in mactelnet.c in the client in MAC-Telnet 0.4.3 and earlier allows remote TELNET servers to execute arbitrary code via a long string in an MT_CPTYPE_PASSSALT control packet.	30/08/2016	7.5	CVE-2016-7115
vbulletin -- vbulletin	SQL injection vulnerability in forumrunner/includes/moderation.php in vBulletin before 4.2.2 Patch Level 5 and 4.2.3 before Patch Level 1 allows remote attackers to execute arbitrary SQL commands via the postids parameter to forumrunner/request.php, as exploited in the wild in July 2016.	30/08/2016	7.5	CVE-2016-6195
vmware -- photon_os	VMware Photos OS OVA 1.0 before 2016-08-14 has a default SSH public key in an authorized_keys file, which allows remote attackers to obtain SSH access by leveraging knowledge of the private key.	30/08/2016	9.3	CVE-2016-5333
vmware -- identity_manger	VMware Identity Manager 2.x before 2.7 and vRealize Automation 7.0.x before 7.1 allow local users to obtain root access via unspecified vectors.	30/08/2016	7.2	CVE-2016-5335
vmware -- vrealize_automation	VMware vRealize Automation 7.0.x before 7.1 allows remote attackers to execute arbitrary code via unspecified vectors.	30/08/2016	7.5	CVE-2016-5336
accellion -- kiteworks_appliance	Accellion Kiteworks appliances before kw2016.03.00 use setuid-root permissions for /opt/bin/cli, which allows local users to gain privileges via unspecified vectors.	26/08/2016	7.2	CVE-2016-5662
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.16, Acrobat and Acrobat Reader DC Classic before 15.006.30172, and Acrobat and Acrobat Reader DC Continuous before 15.016.20039 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-1037, CVE-2016-1063, CVE-2016-1064, CVE-2016-1071, CVE-2016-1072, CVE-2016-1073, CVE-2016-1074, CVE-2016-1076, CVE-2016-1077, CVE-2016-1078, CVE-2016-1080, CVE-2016-1081, CVE-2016-1082, CVE-2016-1083, CVE-2016-1084, CVE-2016-1085, CVE-2016-1086, CVE-2016-1088, CVE-2016-1093, CVE-2016-1095, CVE-2016-1116, CVE-2016-1118, CVE-2016-1119, CVE-2016-1120, CVE-2016-1123, CVE-2016-1124, CVE-2016-1125, CVE-2016-1126, CVE-2016-1127, CVE-2016-1128, CVE-2016-1129, CVE-2016-1130, CVE-2016-4088, CVE-2016-4089, CVE-2016-4090, CVE-2016-4093, CVE-2016-4094, CVE-2016-4096, CVE-2016-4097, CVE-2016-4098, CVE-2016-4099, CVE-2016-4100, CVE-2016-4101, CVE-2016-4103, CVE-2016-4104, and CVE-2016-4105.	26/08/2016	10.0	CVE-2016-4119
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4266, CVE-2016-4267, CVE-2016-4268, CVE-2016-4269, and CVE-2016-4270.	26/08/2016	10.0	CVE-2016-4265
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4267, CVE-2016-4268, CVE-2016-4269, and CVE-2016-4270.	26/08/2016	10.0	CVE-2016-4266
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4266, CVE-2016-4268, CVE-2016-4269, and CVE-2016-4270.	26/08/2016	10.0	CVE-2016-4267
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4266, CVE-2016-4267, CVE-2016-4268, CVE-2016-4269, and CVE-2016-4270.	26/08/2016	10.0	CVE-2016-4268
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4266, CVE-2016-4267, CVE-2016-4268, and CVE-2016-4269.	26/08/2016	10.0	CVE-2016-4269
adobe -- acrobat	Adobe Reader and Acrobat before 11.0.17, Acrobat and Acrobat Reader DC Classic before 15.006.30198, and Acrobat and Acrobat Reader DC Continuous before 15.017.20050 on Windows and OS X allow attackers to execute arbitrary code or cause a denial of service (memory corruption) via unspecified vectors, a different vulnerability than CVE-2016-4191, CVE-2016-4192, CVE-2016-4193, CVE-2016-4194, CVE-2016-4195, CVE-2016-4196, CVE-2016-4197, CVE-2016-4198, CVE-2016-4199, CVE-2016-4200, CVE-2016-4201, CVE-2016-4202, CVE-2016-4203, CVE-2016-4204, CVE-2016-4205, CVE-2016-4206, CVE-2016-4207, CVE-2016-4208, CVE-2016-4211, CVE-2016-4212, CVE-2016-4213, CVE-2016-4214, CVE-2016-4250, CVE-2016-4251, CVE-2016-4252, CVE-2016-4254, CVE-2016-4265, CVE-2016-4266, CVE-2016-4267, CVE-2016-4268, and CVE-2016-4269.	26/08/2016	10.0	CVE-2016-4270
readydesk -- readydesk	SQL injection vulnerability in chat/staff/default.aspx in ReadyDesk 9.1 allows remote attackers to execute arbitrary SQL commands via the user name field.	26/08/2016	7.5	CVE-2016-5048
readydesk -- readydesk	Unrestricted file upload vulnerability in chat/sendfile.aspx in ReadyDesk 9.1 allows remote attackers to execute arbitrary code by uploading and requesting a .aspx file.	26/08/2016	7.5	CVE-2016-5050

Semana 22/08/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
apple -- iphone_os	The kernel in Apple iOS before 9.3.5 allows attackers to obtain sensitive information from memory via a crafted app.	25/08/2016	7.1	CVE-2016-4655
apple -- iphone_os	The kernel in Apple iOS before 9.3.5 allows attackers to execute arbitrary code in a privileged context or cause a denial of service (memory corruption) via a crafted app.	25/08/2016	9.3	CVE-2016-4656
cisco -- anyconnect_secure_mobility_client	Cisco AnyConnect Secure Mobility Client before 4.2.05015 and 4.3.x before 4.3.02039 mishandles pathnames, which allows local users to gain privileges via a crafted INF file, aka Bug ID CSCuz92464.	25/08/2016	7.2	CVE-2016-6369
d-link -- dir-822_firmware	Stack-based buffer overflow in dws/api/Login on D-Link DIR-850L B1 2.07 before 2.07WWB05, DIR-817 Ax, DIR-818LW Bx before 2.05b03beta03, DIR-822 C1 3.01 before 3.01WWb02, DIR-823 A1 1.00 before 1.00WWb05, DIR-895L A1 1.11 before 1.11WWb04, DIR-890L A1 1.09 before 1.09b14, DIR-885L A1 1.11 before 1.11WWb07, DIR-880L A1 1.07 before 1.07WWb08, DIR-868L B1 2.03 before 2.03WWb01, and DIR-868L C1 3.00 before 3.00WWb01 devices allows remote attackers to execute arbitrary code via a lone session cookie.	25/08/2016	9.3	CVE-2016-5681
fortinet -- fortios	Buffer overflow in the Cookie parser in Fortinet FortiOS 4.x before 4.1.11, 4.2.x before 4.2.13, and 4.3.x before 4.3.9 and FortiSwitch before 3.4.3 allows remote attackers to execute arbitrary code via a crafted HTTP request, aka EGREGIOUSBLUNDER.	24/08/2016	10.0	CVE-2016-6909
watchguard -- rapidstream	WatchGuard RapidStream appliances allow local users to gain privileges and execute arbitrary commands via a crafted ifconfig command, aka ESCALATEPLOWMAN.	24/08/2016	7.2	CVE-2016-7089
moxa -- oncell_g3001_firmware	Moxa OnCell G3100V2 devices before 2.8 and G3111, G3151, G3211, and G3251 devices before 1.7 do not properly restrict authentication attempts, which makes it easier for remote attackers to obtain access via a brute-force attack.	23/08/2016	10.0	CVE-2016-5799
rockwellautomation -- 1766-l32awa	Rockwell Automation MicroLogix 1400 PLC 1766-L32BWA, 1766-L32AWA, 1766-L32BXB, 1766-L32BWAA, 1766-L32AWAA, and 1766-L32BXBA devices have a hardcoded SNMP community, which makes it easier for remote attackers to load arbitrary firmware updates by leveraging knowledge of this community.	23/08/2016	7.5	CVE-2016-5645
zmodo -- zp-ibh-13w	ZModo ZP-NE14-S and ZP-IBH-13W devices have a hardcoded root password, which makes it easier for remote attackers to obtain access via a TELNET session.	23/08/2016	10.0	CVE-2016-5081
brocade -- fabric_os	HPE FOS before 7.4.1d and 8.x before 8.0.1 on StoreFabric B switches allows remote attackers to obtain sensitive information via unspecified vectors.	22/08/2016	7.8	CVE-2016-4376
cisco -- ip_phone_8800_series_firmware	Cisco IP Phone 8800 devices with software 11.0(1) allow remote attackers to cause a denial of service (memory corruption) via a crafted HTTP request, aka Bug ID CSCuz03038.	22/08/2016	7.8	CVE-2016-1479
cisco -- ios_xr	Memory leak in Cisco IOS XR 5.1.x through 5.1.3, 5.2.x through 5.2.5, and 5.3.x through 5.3.2 on ASR 9001 devices allows remote attackers to cause a denial of service (control-plane protocol outage) via crafted fragmented packets, aka Bug ID CSCux26791.	22/08/2016	7.8	CVE-2016-6355
cisco -- aironet_access_point_software	Cisco Aironet 1800, 2800, and 3800 devices with software before 8.2.110.0, 8.2.12x before 8.2.121.0, and 8.3.x before 8.3.102.0 allow local users to gain privileges via crafted CLI parameters, aka Bug ID CSCuz24725.	22/08/2016	7.2	CVE-2016-6362
hp -- converged_infrastructure_solution_sizer_suite	HPE Smart Update in Storage Sizing Tool before 13.0, Converged Infrastructure Solution Sizer Suite (CISSS) before 2.13.1, Power Advisor before 7.8.2, Insight Management Sizer before 16.12.1, Synergy Planning Tool before 3.3, SAP Sizing Tool before 16.12.1, Sizing Tool for SAP Business Suite powered by HANA before 16.11.1, Sizer for ConvergedSystems Virtualization before 16.7.1, Sizer for Microsoft Exchange Server before 16.12.1, Sizer for Microsoft Lync Server 2013 before 16.12.1, Sizer for Microsoft SharePoint 2013 before 16.13.1, Sizer for Microsoft SharePoint 2010 before 16.11.1, and Sizer for Microsoft Skype for Business Server 2015 before 16.5.1 allows remote attackers to execute arbitrary code via unspecified vectors.	22/08/2016	7.6	CVE-2016-4377
navis -- webaccess	SQL injection vulnerability in news pages in Cargotec Navis WebAccess before 2016-08-10 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	22/08/2016	7.5	CVE-2016-5817
citrix -- xenapp	Citrix XenApp 6.x before 6.5 HRP07 and 7.x before 7.9 and Citrix XenDesktop before 7.9 might allow attackers to weaken an unspecified security mitigation via vectors related to memory permission.	19/08/2016	7.5	CVE-2016-6493
dbd-mysql_project -- dbd-mysql	Use-after-free vulnerability in DBD::mysql before 4.029 allows attackers to cause a denial of service (program crash) or possibly execute arbitrary code via vectors related to a lost server connection.	19/08/2016	10.0	CVE-2014-9906

Histórico de vulnerabilidades de Agosto do 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_errno after a failure of my_login.	19/08/2016	10.0	CVE-2015-8949
f5 -- big-ip_access_policy_manager	The Configuration utility in F5 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 11.4.x before 11.4.1 HF10, 11.5.x before 11.5.4, and 11.6.x before 11.6.1; BIG-IP AFM and PEM 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 customization configuration section that allows file uploads.	19/08/2016	8.5	CVE-2015-8022

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 commands as root via a crafted upgrade parameter, aka Bug ID CSCux15507.	18/08/2016	8.5	CVE-2016-1365
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 CSCur25513.	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 CSCur25483.	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 IPv4 SNMP packets, aka Bug ID CSCva92151 or EXTRABACON.	18/08/2016	8.5	CVE-2016-6366

Semana 08/08/2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
haxx -- 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 munge_other_line function in cachemgr.cgi in the squid package before 3.1.23-16.el6_8.6 in Red Hat Enterprise Linux 6 allows remote attackers to execute arbitrary code via unspecified vectors. NOTE: this vulnerability exists because of an incorrect fix for CVE-2016-4051.	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-2016-3290.	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-2016-3322.	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-2016-3293
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-2016-3300
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; Windows 10 Gold, 1511, and 1607; Office 2007 SP3; Office 2010 SP2; 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-2016-3301
microsoft -- live_meeting	The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Office 2007 SP3, Office 2010 SP2, 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-2016-3304.	09/08/2016	9.3	CVE-2016-3303
microsoft -- live_meeting	The Windows font library in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Office 2007 SP3, Office 2010 SP2, 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-2016-3303.	09/08/2016	9.3	CVE-2016-3304
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-2016-3309, CVE-2016-3310, and CVE-2016-3311.	09/08/2016	7.2	CVE-2016-3308
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-2016-3309
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-2016-3310
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-2016-3310.	09/08/2016	7.2	CVE-2016-3311
microsoft -- office	Microsoft Office 2007 SP3, 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-2016-3313
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-2016-3316
microsoft -- office	Microsoft Office 2010 SP2, Word 2007 SP3, 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-2016-3317
microsoft -- office	Microsoft Office 2007 SP3, 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-2016-3318
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	9.3	CVE-2016-3319
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-2016-3289.	09/08/2016	7.6	CVE-2016-3322
cisco -- rv110w_wireless-n_vpn_firewall_firmware	The CLI command parser on Cisco RV110W, RV130W, and RV215W devices allows local users to execute arbitrary shell commands as an administrator via crafted parameters, aka Bug IDs CSCuv90134, CSCux58161, and CSCux73567.	07/08/2016	7.2	CVE-2015-6396
cisco -- rv110w_wireless-n_vpn_firewall_firmware	Cisco RV110W, RV130W, and RV215W devices have an incorrect RBAC configuration for the default account, which allows remote authenticated users to obtain root access via a login session with that account, aka Bug IDs CSCuv90139, CSCux58175, and CSCux73557.	07/08/2016	9.0	CVE-2015-6397
cisco -- rv180_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 CSCuz43023.	07/08/2016	7.8	CVE-2016-1429
cisco -- rv180_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 CSCuz48592.	07/08/2016	9.0	CVE-2016-1430
cisco -- unified_communications_manager	Cisco Unified Communications Manager IM and Presence Service 9.1(1) SU6, 9.1(1) SU6a, 9.1(1) SU7, 10.5(2) SU2, 10.5(2) SU2a, 11.0(1) SU1, and 11.5(1) allows remote attackers to cause a denial of service (sipd process restart) via crafted headers in a SIP packet, aka Bug ID CSCva39072.	07/08/2016	7.8	CVE-2016-1466
cisco -- ios	Cisco IOS 15.5(3)S3, 15.6(1)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 wedge) by sending many crafted NTP packets, aka Bug ID CSCva35619.	07/08/2016	7.8	CVE-2016-1478
google -- chrome	Heap-based buffer overflow in the opj_j2k_read_SQcd_SQcc function in j2k.c in OpenJPEG, as used in PDFium 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 remoteFrontendUrl 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 remoteFrontendUrl 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 -- qradar_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-2016-2875
linux -- linux_kernel	The vfe31_proc_general function in drivers/media/video/msm/vfe/msm_vfe31.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-2014-9410
linux -- linux_kernel	Use-after-free vulnerability in the msm_set_crop function in drivers/media/video/msm/msm_camera.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-2015-0568
linux -- linux_kernel	drivers/media/platform/msm/broadcast/tsc.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_GET_CARD_STATUS ioctl call.	07/08/2016	10.0	CVE-2015-0573
linux -- linux_kernel	Stack-based buffer overflow in the supply_lm_input_write function in drivers/thermal/supply_lm_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	sound/soc/msm/qdsp6v2/msm-audio-effects-q6-v2.c in the MSM QDSP6 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/soc/msm/qdsp6v2/msm-audio-effects-q6-v2.c in the MSM QDSP6 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 triggering incorrect use of a parameters pointer.	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 KGSL Linux Graphics Module, which allows attackers to bypass intended access restrictions by using the /ashmem string as the dentry name.	07/08/2016	7.2	CVE-2016-5340
moxa -- softcms	SQL injection vulnerability in Moxa SoftCMS before 1.5 allows remote attackers to execute arbitrary SQL commands via unspecified fields.	07/08/2016	7.5	CVE-2016-5792

Histórico de vulnerabilidades de Agosto do 2016

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
openbsd -- openssh	The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.	07/08/2016	7.8	CVE-2016-6515
php -- php	Multiple integer overflows in php_zip.c in the zip 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) getFromIndex or (2) getFromName in the ZipArchive class.	07/08/2016	7.5	CVE-2016-3078
php -- php	Double free vulnerability in the SplDoublyLinkedList::offsetSet function in ext/spl/spl_dllist.c 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 get_icu_value_internal function in ext/intl/locale/locale_methods.c 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 locale_get_primary_language call.	07/08/2016	7.5	CVE-2016-5093
php -- php	Integer overflow in the php_html_entities function in ext/standard/html.c 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 the htmlspecialchars function.	07/08/2016	7.5	CVE-2016-5094
php -- php	Integer overflow in the php_escape_html_entities_ex function in ext/standard/html.c 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 FILTER_SANITIZE_FULL_SPECIAL_CHARS filter_var call. 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 fread function in ext/standard/file.c 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 large integer in the second argument.	07/08/2016	7.5	CVE-2016-5096
php -- php	Double free vulnerability in the _php_mb_regex_ereg_replace_exec function in php_mbregex.c in the mbstring 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-2016-5768
php -- php	Multiple integer overflows in mcrypt.c in the mcrypt 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) mcrypt_generic and (2) mdecrypt_generic functions.	07/08/2016	7.5	CVE-2016-5769
php -- php	Integer overflow in the SplFileObject::fread function in spl_directory.c in the SPL 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 areument. a related issue to CVE-2016-5096.	07/08/2016	7.5	CVE-2016-5770
php -- php	spl_array.c in the SPL extension in PHP before 5.5.37 and 5.6.x before 5.6.23 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data.	07/08/2016	7.5	CVE-2016-5771
php -- php	Double free vulnerability in the php_wddx_process_data function in wddx.c in the WDDX 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 crafted XML data that is mishandled in a wddx_deserialize call.	07/08/2016	7.5	CVE-2016-5772
php -- php	php_zip.c in the zip extension in PHP before 5.5.37, 5.6.x before 5.6.23, and 7.x before 7.0.8 improperly interacts with the unserialize implementation and garbage collection, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and application crash) via crafted serialized data containing a ZipArchive object.	07/08/2016	7.5	CVE-2016-5773
siemens -- sinema_server	Siemens SINEMA Server uses weak permissions for the application folder, which allows local users to gain privileges via unspecified vectors.	07/08/2016	7.2	CVE-2016-6486
google -- android	Integer underflow in the diag 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 CR549470.	06/08/2016	9.3	CVE-2014-9863
google -- android	drivers/misc/qseecom.c 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 CR561841.	06/08/2016	9.3	CVE-2014-9864
google -- android	drivers/misc/qseecom.c 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 CR550013.	06/08/2016	9.3	CVE-2014-9865
google -- android	drivers/media/platform/msm/camera_v2/sensor/csid/msm_csid.c 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 28747684 and Qualcomm internal bug CR511358.	06/08/2016	9.3	CVE-2014-9866
google -- android	drivers/media/platform/msm/camera_v2/isp/msm_isp_axi_util.c 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-2014-9867
google -- android	drivers/media/platform/msm/camera_v2/isp/msm_isp_stats_util.c 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 CR514711.	06/08/2016	9.3	CVE-2014-9869
google -- android	The Linux kernel before 3.11 on ARM platforms, as used in Android before 2016-08-05 on Nexus 5 and 7 (2013) devices, does not properly consider user-space access to the TPIDRURW register, which allows local users to gain privileges via a crafted application, aka Android internal bug 28749743 and Qualcomm internal bug CR561044.	06/08/2016	9.3	CVE-2014-9870
google -- android	Multiple buffer overflows in drivers/media/platform/msm/camera_v2/isp/msm_isp_util.c 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-2014-9871
google -- android	drivers/misc/qseecom.c 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 CR616633.	06/08/2016	9.3	CVE-2014-9887
google -- android	Off-by-one error in drivers/media/platform/msm/camera_v2/sensor/cci/msm_cci.c 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 28770207 and Qualcomm internal bug CR529177.	06/08/2016	9.3	CVE-2014-9890
google -- android	drivers/misc/qseecom.c 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-2014-9891
google -- android	The MSM camera driver in the Qualcomm components in Android before 2016-08-05 on Nexus 6 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-2015-8938
google -- android	drivers/video/msm/mdp4_util.c in the Qualcomm components in Android before 2016-08-05 on Nexus 7 (2013) devices does not validate r stages, g stages, or b stages data, which allows attackers to gain privileges via a crafted application, aka Android internal bug 28398884 and Qualcomm internal bug CR779021.	06/08/2016	9.3	CVE-2015-8939
google -- android	Integer overflow in sound/soc/msm/qdsp6v2/q6lsm.c 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 28813987 and Qualcomm internal bug CR792367.	06/08/2016	9.3	CVE-2015-8940
google -- android	drivers/media/platform/msm/camera_v2/isp/msm_isp_axi_util.c 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 28814502 and Qualcomm internal bug CR792473.	06/08/2016	9.3	CVE-2015-8941
google -- android	drivers/media/platform/msm/camera_v2/pproc/cpp/msm_cpp.c 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 28814652 and Qualcomm internal bug CR803246.	06/08/2016	9.3	CVE-2015-8942
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 (use-after-free and system crash) via a crafted sendmsg system call.	06/08/2016	7.2	CVE-2016-3841
linux -- linux_kernel	arch/arm/mm/dma-mapping.c in the Linux kernel before 3.13 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 28803642 and Qualcomm internal bug CR642735.	06/08/2016	7.2	CVE-2014-9888
linux -- linux_kernel	The apparmor_setprocattr function in security/apparmor/lsm.c in the Linux kernel before 4.6.5 does not validate the buffer size, which allows local users to gain privileges by triggering an AppArmor setprocattr hook.	06/08/2016	7.2	CVE-2016-6187
dashbuilder_project -- dashbuilder	SQL injection vulnerability in the getStringParameterSQL method in main/java/org/dashbuilder/dataprovider/sql/dialect/DefaultDialect.java in Dashbuilder before 0.6.0.Beta1 allows remote attackers to execute arbitrary SQL commands via a data set lookup filter in the (1) Data Set Authoring or (2) Displayer 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 snprintf 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-2014-9901
google -- android	Buffer overflow in CORE/SYS/legacy/src/utils/src/dot11f.c 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 bugs CR553931 and CR553941.	05/08/2016	10.0	CVE-2014-9902
google -- android	services/core/java/com/android/server/pm/PackageManagerService.java 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 27450489.	05/08/2016	7.5	CVE-2016-2497
google -- android	Integer overflow in codecs/on2/h264dec/source/h264bsd_dpb.c in libstagefright 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 2016-08-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted media file, aka internal bug 28533562.	05/08/2016	7.5	CVE-2016-3819
google -- android	The ih264d decoder in mediaserver in Android 6.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 28673410.	05/08/2016	7.5	CVE-2016-3820
google -- android	libmedia 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 2016-08-01 has certain 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 28166152.	05/08/2016	7.5	CVE-2016-3821
google -- android	exif.c in Matthias Wandel jhead 2.87, as used in libjhead 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 crafted EXIF data. aka internal bug 28868315.	05/08/2016	7.5	CVE-2016-3822
google -- android	codecs/hevcdec/SoftHEVC.cpp in libstagefright in mediaserver 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/ih264d_api.c in mediaserver 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 ih264d decoder in mediaserver 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 29023649.	05/08/2016	7.1	CVE-2016-3829
google -- android	codecs/aacdec/SoftAAC2.cpp in libstagefright 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 2016-08-01 allows remote attackers to cause a denial of service (device hang or reboot) via crafted ADTS data, aka internal bug 29153599.	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 Package Manager, which allows attackers to bypass an unspecified protection mechanism via a crafted application, aka internal bug 28795098.	05/08/2016	8.3	CVE-2016-3832
google -- android	The Shell component 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 MANAGE_USERS and CREATE_USERS 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	Conscrypt 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 28377352 and Qualcomm internal bug CR1002974.	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 bugs 28086229 and 29119870 and Qualcomm internal bug CR1011071.	05/08/2016	9.3	CVE-2016-3843
google -- android	mediaserver 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 28299517.	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 28817378.	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

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	9.3	CVE-2016-3851
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 28522518.	05/08/2016	9.3	CVE-2016-3857
juniper -- junos	Juniper Junos OS before 12.1X46-D50, 12.1X47 before 12.1X47-D23, 12.3X48 before 12.3X48-D25, 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 flip-flop failovers) 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 2233550.	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 2234226.	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 45.3 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-2016-5254
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 5.12.x before 5.12.3.1 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-2016-5229
citrix -- xenserver	The PV pagetable code in arch/x86/mm.c in Xen 4.7.x and earlier allows local 32-bit PV guest OS administrators to gain host OS privileges by leveraging fast-paths for updating pagetable entries.	02/08/2016	7.2	CVE-2016-6258
crestron -- airmedia_am-100_firmware	Directory traversal vulnerability in cgi-bin/rftest.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-txrx-100-str_firmware	Crestron Electronics DM-TXRX-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-txrx-100-str_firmware	Crestron Electronics DM-TXRX-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-txrx-100-str_firmware	Crestron Electronics DM-TXRX-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 CX600 devices with software before V800R007SPH017; PTN 6900-2-M8 devices with software before V800R007SPH019; NE5000E devices with software before V800R006SPH018; and CloudEngine devices 12800 with software before V100R003SPH010 and V100R005 before V100R005SPH006 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-2016-6178
huawei -- p8_smartphone_firmware	Buffer overflow in the Wi-Fi driver in Huawei P8 smartphones with software before GRA-CL00C92B363 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-CL00C92B363 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/vainit.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/ptargrep, (4) cpan/CPAN/scripts/cpan, (5) cpan/Digest-SHA/shasum, (6) cpan/Encode/bin/enc2xs, (7) cpan/Encode/bin/encguess, (8) cpan/Encode/bin/piconv, (9) cpan/Encode/bin/ucmlint, (10) cpan/Encode/bin/unidump, (11) cpan/ExtUtils-MakeMaker/bin/instmodsh, (12) cpan/IO-Compress/bin/zipdetails, (13) cpan/JSON-PP/bin/json_pp, (14) cpan/Test-Harness/bin/prove, (15) dist/ExtUtils-ParseXS/lib/ExtUtils/xsubpp, (16) dist/Module-CoreList/corelist, (17) ext/Pod-Html/bin/pod2html, (18) utils/c2ph.PL, (19) utils/h2ph.PL, (20) utils/h2xs.PL, (21) utils/libnetcfg.PL, (22) utils/perlbug.PL, (23) utils/perldoc.PL, (24) utils/perlivp.PL, and (25) utils/splain.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
pulsesecure -- odyssey_access_client	An unspecified client-side component in Pulse Secure Desktop Client before 5.0r15.1, 5.1rX before 5.1r9.1, and 5.2rX before 5.2r4.1; Installer Service (formerly Juniper Installer Service) and Collaboration (formerly Secure Meeting) before 8.0r15.1, 8.1rX before 8.1r9.1, and 8.2rX before 8.2r4.1; 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-2016-2408
redhat -- jboss_operations_network	The server in Red Hat JBoss Operations Network (JON) before 3.3.6 allows remote attackers to execute arbitrary code via a crafted HTTP request, related to message deserialization.	02/08/2016	9.0	CVE-2016-3737
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-2016-4373
novell -- filr	vaconfig/time 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 ntpServer parameter.	31/07/2016	9.0	CVE-2016-1608